amendment No. 1052 proposed to H.R. 2361, supra.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. LOTT (for himself and Mr. BAUCUS):

S. 1327. A bill to amend the Internal Revenue Code of 1986 to modify the active business definition under section 355; to the Committee on Finance.

Mr. LOTT. Mr. President, I rise today to introduce legislation proposing a change to the Internal Revenue Code that has been endorsed by both the Joint Committee on Taxation and the United States Treasury Department. It is a simplification measure that has been passed by this body on three separate occasions, and I am pleased to be joined by the gentleman from Montana, Senator BAUCUS, the Ranking Democratic Member on the Finance Committee, in introducing this common sense legislation today. It is now time for Congress to act again and include this meritorious provision in the next appropriate tax bill reported from the Finance Committee.

Corporations and affiliated groups of corporations, for any number of good reasons, find it appropriate and many times necessary to shed some of their businesses. If the business is not being sold, the Internal Revenue Code makes it possible to reorganize without having to recognize gain on the transaction. A typical transaction is a spin-off transaction performed per the terms of section 355 of the Internal Revenue Code, where a parent corporation distributes the shares of its subsidiary(s) to its shareholders who once had shares of just the parent corporation now have shares of both the parent and the shares of just the parent corporation now have shares of its subsidiary(s) to its shareholders who once had shares of just the parent corporation now have shares of both the parent and the subsidiary. As a matter of long-standing tax policy, there is typically no tax exacted with these kinds of divisions, nor should there be. Typically the business hasn't changed what it is doing; it is simply being done under a separated ownership structure and the shareholders have ownership in two corporations instead of one, with no overall change in their holdings.

In order to be accorded tax-free treatment, section 355 requires the corporation involved in the transaction to be engaged in an ''active trade or business.'' Under the current regulations interpreting section 355 of the Internal Revenue Code, a much more rigorous test of ''active trade or business'' is imposed if a holding company seeks to spin-off a subsidiary than would be the case if the subsidiary were simply owned directly by the parent corporation. It is a distinction without substance and requires corporations, holding companies, to go through major restructurings to satisfy the requirements of section 355. There is absolutely no substantive policy rationale for such a result. The distinction is inappropriate and has been identified as such by both the staff of the Joint Committee on Taxation and the Treasury Department in 1999 and 2000. This legislation addresses that anomaly and treats both situations equally.

The cost of this provision is minimal, at about $8 million a year by the last revenue estimate from the staff of the Joint Committee on Taxation. This provision is a small but significant step toward simplification of the tax code, and I urge my colleagues on the Finance Committee and in this body to act on this change one more time, and hopefully for the last time.

Mr. BAUCUS. Mr. President, virtually everyone supports tax simplification. But for some reason, it is awfully hard to accomplish. Today, I am pleased to join my friend and colleague from Mississippi, Senator LOTT, in introducing tax legislation that is non-controversial and a clear tax simplification measure. Further, the bill we are filing today has been supported in the past by the Joint Tax Committee and the U.S. Treasury.

Normally, corporations are taxed on distributions of property to shareholders as if sold at fair market value. However, section 355 of the tax code provides corporations with the flexibility to distribute one or more of their businesses to their shareholders, such as in a spin-off, without triggering tax consequences if the transaction meets important requirements. Through this exception in section 355, corporations may make strategic business decisions without imposing tax burdens on their shareholders, but only if both the distributing and distributed businesses continue as an active trade or business. The regulatory structure that has evolved over the years under section 355 has created very different ''active trade or business'' tests depending on whether the distributing corporation operates as a holding company or whether it holds the business assets directly. There is no rationale to support that distinction.

Both the staff of the Joint Tax Committee and the Clinton Treasury Department recommended that the rules be conformed as a tax simplification measure. The Senate has passed legislation similar to what we are proposing today on three occasions. And, on one of those occasions, it passed the House as well in legislation that was later vetoed for other reasons. I have heard of no opposition to this change, which would simply apply a ''look through'' rule for the ''active trade or business'' test on an affiliated group level, so that parent holding companies could count the active businesses of its subsidiaries. And it would eliminate hours of wasted time and resources in tax planning activities that serve no function other than to try and conform corporate ownership structures to satisfy the literal language of current tax requirements.

Again, I should emphasize that this proposal does not bring wholesale change to section 355. Spin-off requirements dealing with the continuity of historical shareholder interest, continuity of business enterprises, business purpose, and absence of any device to distribute earnings and profits all remain. With a cost of less than $10 million a year, this is an affordable step we can take now to simplify the Internal Revenue Code.

I am pleased to join with Senator LOTT in working for passage of this important simplification bill, and I urge my colleagues on the Finance Committee and in the Senate give our bill every consideration.

By Mr. JEFFORDS (for himself and Mr. SARBANES):

S. 1328. A bill to amend the Safe Drinking Water Act to ensure that the District of Columbia and States are provided a safe, lead-free supply of drinking water; to the Committee on Environment and Public Works.

Mr. JEFFORDS. Mr. President, I rise today to introduce the Lead-Free Drinking Water Act of 2005 with my colleague Senator SARBANES. We are joined by our colleagues, Congresswoman NORTON, Congressman WAXMAN, and others, who will be introducing the House companion bill today. Today, we introduce this bill for the second time.

Last year, we shared the shock felt by DC residents when it was first reported that lead levels in the DC public water system were significantly higher than Federal guidelines, and had been so for at least 2 years.

We sought answers to the same questions everyone was asking themselves—How much water did I drink? How much water did my children drink? What are the effects of lead in our bloodstream?

We shared the outrage felt by many DC residents, asking ourselves—why were we not told about this sooner? How did this happen? What are we going to do about it?

In the 108th Congress, we attempted to answer those questions. We held a hearing in the Senate Environment and Public Works Committee and listened to the concerns of DC parents worried about their children's health.

We listened to experts who identified weaknesses in the Safe Drinking Water Act and the lead and copper rule, governing how the public is informed when lead is present in a drinking water system and what corrective actions public water systems must take.

One of the most disturbing points is that many of the things that happened in Washington, DC, were within the boundaries of the existing rules that purport to protect the public from lead in drinking water.

We responded by introducing the Lead-Free Drinking Water Act of 2004, which sought to correct the weaknesses in those rules.

Today, we are reintroducing the Lead-Free Drinking Water Act of 2005.

Our bill will overhaul the Safe Drinking Water Act to strengthen the Federal rules governing lead testing and regulations in our public water systems to ensure that our most vulnerable citizens—infants, children, pregnant women, and new moms—are not harmed by lead in drinking water.

Specifically, the bill requires the EPA to reevaluate the current regulatory structure to figure out if it really provides the level of public health protection required.

The bill calls on the EPA to establish a maximum contaminant level for lead at the tap, and if that is not practical given the presence of lead inside home plumbing systems, the bill requires EPA to reevaluate the current action level for lead to ensure that vulnerable populations such as infants, children, pregnant women, and nursing mothers receive adequate protection.

I look forward to working with EPA on this evaluation to determine which approach is most feasible and which provides the greatest level of public health protection.

EPA has three choices: keep current standard, an ''action level'' at 15 parts per billion; lower the current action level below 15 parts per billion; establish a ''maximum contaminant load.''

For example, it is clear that a maximum contaminant level, which is measured at the water treatment plant, would do little to protect people from lead-contaminated drinking water at their faucets. Our bill requires that standards be measured at the tap.

A low lead action level measured at the tap could provide more protection than a high MCL measured anywhere in the system if there were extremely strong and effective public notification procedures in place.

Public notice is the key to success of any lead regulation—parents say to me, ''If only I had known, I could have protected my family.'' It is our job to be sure the public notice system we have in place gets people the information they need when they need it.

The bill will require information such as the number of homes tested, the lead levels found, the areas of the community in which they were located, and the disproportionate adverse health effects of lead on infants, be made public immediately upon detection of lead.

In addition, the bill requires that, as part of routine testing conducted, any residents whose homes test high for lead receive notification and appropriate medical referrals within 14 days.

Finally, we don't want the day of an exceedance to be the first time people have heard about lead in drinking water. The bill establishes a basic public education program to ensure that people have a basic understanding that lead may be present in drinking water and what the corrective actions might be even before their water system detects a problem.

The bill requires increased water testing and lead remediation in schools and day-care centers nationwide. This provision exists in law today, but it was affected by previous litigation. This bill corrects the problem by requiring the Administrator to execute this program if states choose not to. It is wholly unacceptable to do anything less than provide a learning environment for our next generation that does not degrade their intellectual capacity. Our bill provides $150 million over 5 years for this program.

And we strengthen existing requirements to ensure that all lead service lines will be replaced by a public water system at a rate of 10 percent per year until they are gone.

This is common sense—let us get rid of the lead in our systems and get rid of the lead in our water.

Our bill makes water systems responsible for replacing lead service lines, including the privately owned sections, once a system exceeds lead standards. Homeowners have the final say in whether their line is replaced.

We provide $1 billion over 5 years for lead service line replacement.

The EPA estimates that our Nation needs $265 billion to maintain and improve its drinking water infrastructure over the next 20 years.

If we do not address this, we will be facing more and more health and environmental issues as our Nation's water infrastructure degrades.

Lead service lines are only one part of the picture. Leaded solder was banned in 1987. However, ''lead-free'' plumbing fixtures are currently allowed to have 8 percent lead.

Our bill makes ''lead-free'' mean lead-free. It defines the term as trace amounts of lead −0.2 percent. It prohibits the use of pipes, or pipe or plumbing fitting or fixtures that are ''high lead'' which our bill defines as 2.0 percent lead within 1 year. And within 5 years, it prohibits the use of any plumbing components with anymore than 0.2 percent lead. This is a huge step toward making our water systems truly lead-free.

Our bill strengthens existing requirements for leaching by requiring independent third-party performance certification.

Finally, our bill requires that the existing requirements for leaching be revised to be as protective as the existing leaching standards in California which have set the bar for plumbing fittings and fixtures.

We urge our colleagues to support this legislation.

Last year, Good Housekeeping independently ran a piece about the Lead-Free Drinking Water Act and gave its readers information to contact us with their support. We received over a thousand responses from individual readers in 48 States and the District of Columbia.

In the 18th century, almost 300 years ago, Ben Franklin concluded that lead was poisonous. In a biography written by Edmund S. Morgan, this story is recounted:

At the request of his friend and English publisher Benjamin Vaughan, he wrote out a proof of what he had once casually mentioned in conversation: his conclusion that lead was poisonous. After detailing his own and other printers' ailments from the continuous handling of lead type, he went on to describe his observations of the grass and plants that died from the fumes near furnaces where lead was smelted, of the effects of drinking rainwater that sluiced off lead roofs, and of his queries to sickened plumbers, painters, and glaziers in a Paris hospital. His observations of the toxic effects of lead, he noted, were nothing new; and he remarked wryly, ''how long a useful Truth may be known, and exist, before it is generally receiv'd and practis'd on.''

We have known lead is a poison for centuries. What are we waiting for? As we learned from the incidents in Washington, DC, and Boston, there are large deficiencies in Federal safe drinking water regulations. It is time to plug the holes in these regulations and fully protect the public from this poison. It is time to get the lead out.

Safe drinking water is not a privilege; it is a right—whether you live in Washington, DC, or Washington State or Washington County, VT.

I urge my colleagues to join us in working to pass the Lead-Free Drinking Water Act of 2005 to get the lead out of our pipes, out of our water, out of our families, and out of our lives.

By Mrs. CLINTON (for herself, Mr. SMITH, Mr. MARTINEZ, Mr. REED, and Mr. DURBIN):

S. 1330. A bill to amend the Internal Revenue Code of 1986 to provide incentives for employer-provided employee housing assistance, and for other purposes; to the Committee on Finance.

Mrs. CLINTON. Mr. President, I rise today during National Home Ownership Month to introduce the Housing America's Workforce Act.

Affordable and safe housing plays a vital role in creating and sustaining healthy communities and a vibrant workforce. The Housing America's Workforce Act creates incentives to expand employer-assisted housing initiatives across the Nation. I thank Senators SMITH, MARTINEZ, REED, and DURBIN for their co-sponsorship of this important legislation. I would also like to thank Congresswoman NYDIA VELÁZQUEZ for her leadership in introducing the companion bill in the House of Representatives.

The sad truth is that across our Nation, working full-time no longer guarantees that a family will be able to afford a secure and comfortable home. The shortage of workforce housing has become a national crisis as housing costs have far outgrown the rate of inflation in many markets and as the gap between wages and housing costs widens. The result is that affordable housing is out of reach for a growing number of working families. As a result,

people who provide the backbone services for our communities—teachers, firefighters, police officers, and nurses—often cannot afford to live in the communities in which they serve. A recent workforce housing study released by the National Association of Home Builders found that for the most part, workers who provide these vital community services can only find housing they can afford in less than half of the nation's top 25 metropolitan areas.

Across the Nation, the number of working families with critical housing problems (defined as those paying more than half of their income for housing and/or living in dilapidated conditions) has increased by 67 percent between 1997 and 2003 to approximately 5 million families. Families that spend more than half of their income on housing have little income left over for other essentials such as food, healthcare, and transportation.

And despite overall improvements in home-ownership trends since 1978, working families—employed households with children earning less than 120 percent of Area Median Income—have actually experienced a decrease in homeownership rates. A 2004 Center for Housing Policy study shows that the homeownership rate for working families with children was at 62.5 percent in 1978, and only 56.6 percent through 2001.

Employer-assisted housing, EAH, is a local, innovative solution that a growing number of employers are using to meet the housing needs of their employees while increasing the competitiveness of their businesses. There are several types of EAH products, including homebuyer education, down payment assistance, rental assistance and loan guarantee programs. Employers often combine these products to meet their employees' specific needs in the most effective ways.

The benefits for employees and employers are impressive. The employee, in addition to receiving financial support from an employer to buy or rent a home closer to work, also regains extra time—formerly spent in traffic—for family or community life. The employer likewise benefits from a more stable workforce when employees live near work. They enjoy the advantages from the improved employee morale, lower turnover rate and reduced recruitment costs result in bottom line savings that the increased proximity brings. Furthermore, EAH programs benefit not only the workers and employers, but also the entire community. As former commuters buy homes near the jobsite, the surrounding community which previously suffered from traffic congestion, now enjoys new investment and property tax revenues.

The Housing America's Workforce Act is inspired in great part by lessons learned in States and local communities across the Nation, where EAH has proven to be an effective tool to promote housing affordability for working families and community revitalization. Through EAH programs, the private sector becomes part of the solution, investing in housing assistance for employees while experiencing bottom line benefits. This is clearly a public-private partnership that is proven and makes sense.

The Housing America's Workforce Act provides incentives to increase private sector investment in housing in three important ways. First, it offers a tax credit of 50 cents for every dollar that an employer provides to eligible employees up to $10,000 or six percent of the employee's home purchase price, whichever is less, or up to $2,000 for rental assistance. Second, to ensure that employees receive the full value of employers' contributions, the Act defines housing assistance as a ''nontaxable benefit,'' similar to health, dental and life insurance. Third, the act establishes a competitive grant program available to nonprofit housing organizations that provide technical assistance, program administration, and outreach support to employers undertaking EAH initiatives.

In New York and in other parts of the country, EAH has caught on with the local business community, elected and appointed officials, and the broader housing arena. Its expansion indicates a growing understanding among the private sector that it pays to invest in workforce housing. I have worked with employers across my State to launch county employer-assisted housing programs in places such as Long Island, Rochester and Westchester.

I have met many of the families that have already benefited from Long Island's EAH program, which I helped launch in 2002. People like the Isaacs family, who were able to buy their first home in North Amityville in 2002 thanks to their employer's participation in the program. Pamela Isaac, like so many employees on Long Island, works as a Dietician at Our Lady of Consolation, part of the Catholic Health Services Network. Catholic Health Services' participation in the employer assisted housing program enabled Pamela and her husband Bartholomew to stay on Long Island and raise their three children in their own home.

I also worked in collaboration with Mayor William A. Johnson of Rochester to jumpstart the City of Rochester's EAH initiative. The City provides $3,000 for its own employees and also encourages other employers to provide a home purchase benefit by offering to match that benefit dollar for dollar up to a maximum of $3,000. Therefore, if an employer offered the maximum benefit of $3,000, he or she would produce a $6,000 benefit for his or her employees with the city's matching funds.

The Westchester County EAH, which was spEAHheaded by the Business Council and Fannie Mae, brings together the following Westchester County nonprofit organizations: Housing Action Council, Westchester Residential Opportunities, Westchester Housing Fund and Community Housing Innovations. Each of these nonprofits provides standardized, comprehensive education and counseling support to participating employers. The initiative also provides matching funds of up to $3,000 from Westchester County or from the cities of Yonkers, New Rochelle, White Plains or Mount Vernon. In addition, the nonprofit collaborative offers down payment and closing cost assistance programs that can match employer contributions.

The creation of Federal incentives to expand employer-assisted housing has been a consistent recommendation of experts in the broader housing arena, including the Millennial Housing Commission. In addition, former HUD Secretaries Henry Cisneros and Jack Kemp, along with Nic Retsinas and Kent Colton of the Harvard Joint Center for Housing Studies recently released a bipartisan platform for national housing policy, which includes EAH as one of its recommendations.

According to the Society for Human Resources Management's 2004 Benefits Survey, 12 percent of employers offered home ownership assistance in 2004, up from 7 percent in 2002. Since 1991, Fannie Mae has offered a nationwide EAH program through participating lending institutions and employers. Fannie Mae has helped about 750 employers of various sizes implement EAH programs and nearly 570 have been launched since 2000. Freddie Mac launched a similar national program in 1999, which it expanded in 2004. Several states have enacted EAH tax incentive programs, including Illinois, Connecticut, Missouri, and New Jersey.

Employer-assisted housing programs offer a fresh approach to addressing our Nation's housing challenge by allowing the private sector to play a direct role in promoting housing affordability. I hope every Senator will recognize that the Housing America's Workforce Act will create opportunities for us as a Nation to expand these public-private partnerships and will make a profound impact in the lives of our workforce, and I hope that you will support this important piece of legislation.

Mr. SMITH. Mr. President, I rise today to join Senators CLINTON, MARTINEZ, REED, and DURBIN to introduce the Housing America's Workforce Act.

Across the country, low- and moderate-income families face difficulty finding affordable housing. Homebuilding has not kept pace with job growth, and the cost of housing has skyrocketed. In the last 5 years, the number of working U.S. families paying more than half their income to put a roof over their heads has jumped to 4.2 million in 2003 from 2.4 million in 1997, a 76-percent increase in 5 years.

Our bill tries to address the issue of affordable housing from a new perspective, one that allows the private sector to play a direct role in promoting housing affordability. Specifically, our bill would create a Federal tax credit for

businesses that offer housing assistance programs to their low- to moderate-income employees.

Employer assisted housing, EAH, programs have been used successfully for more than 100 years and have proven effective in helping to revitalize neighborhoods and to recruit and retain employees. In my home State of Oregon, EAH programs have been used by employers such as Legacy Emanuel Hospital & Health Center, Housing Authority of Portland, Multnomah County, and Wacker Siltronic.

In 1990, Legacy Emanuel developed an EAH program to encourage employees to purchase homes in the neighborhood near the hospital. The program shortened employee commute time, reduced traffic congestion, and helped spur a dramatic revitalization of the surrounding area. Similar programs have succeeded around the country and have helped to ease the spatial mismatch between where job growth is taking place and where people can afford to live.

Under our bill, housing assistance can be used for either homeownership or rental assistance. Homeownership assistance could be used for down payments, closing costs, financing costs, or contributions to an employee homeownership savings plan, such as an Individual Development Accounts. Rental assistance could be used for security deposits and rental payments.

Employer assisted housing programs are innovative ways to leverage public and private funds to make housing affordable for working families. As such, our proposal has been endorsed by National Housing Conference, National Association of Home Builders, National Association of Realtors, National Association of Housing and Redevelopment Officials, National League of Cities, National Association of Counties, Mortgage Bankers Association, National NeighborWorks Association, AmeriDream, and the National Association of Local Housing Finance Agencies.

I look forward to continuing to work with my colleagues to address the affordable housing shortfall.

By Mr. JOHNSON (for himself, Mr. THOMAS, Mr. ENZI, Mr. DORGAN, Mr. BURNS, Mr. THUNE, Mr. BINGAMAN, and Mr. BAUCUS):

S. 1331. A bill to amend the Agricultural Marketing Act of 1946 to change the date of implementation of country of origin labeling to January 30, 2006; to the Committee on Agriculture, Nutrition, and Forestry.

Mr. JOHNSON. Mr. President, I rise to discuss an issue of great importance to producers and consumers in my home State of South Dakota and across the Nation. Mandatory country of origin labeling, COOL, remains an overwhelmingly popular provision not only as a consumer right-to-know issue, but also as a marketing tool for our Nation's farmers and ranchers.

Mandatory country of origin labeling was signed into law under this most recent Farm Bill and by this current President. As the primary author of the COOL language included in the 2002 Farm Bill, I am increasingly frustrated at the amount of heel dragging this Administration has shown for the program. I rise to introduce a bill to move forward with the implementation of mandatory COOL in a timely and reasonable manner, instating a January 30, 2006 mandatory date of implementation. COOL has experienced great bipartisan support in the Senate. I am pleased that Senator CRAIG THOMAS joins me in this bipartisan effort, as does Senator MIKE ENZI, Senator BYRON DORGAN, and Senator CONRAD BURNS.

I worked with my Senate colleagues to ensure that no delay language was included in the Senate version of the fiscal year 2006 Agriculture Appropriations Bill that was reported out of committee. As a member of the Senate Appropriations Committee, and specifically, the Agriculture Appropriations Subcommittee, I worked with my Senate colleagues to ensure we assembled a satisfactory bill that did not contain the same delay language as found in the House agriculture spending measure. The House fiscal year 2006 Agriculture Appropriations Bill contained a 1-year delay for meat and meat products, which is identical to the situation that unfolded with the program in fiscal year 2004.

While the House version of the fiscal year 2004 spending bill contained a 1-year delay for meat and meat products exclusively, the final omnibus contained a 2-year delay for all covered commodities except fish and shellfish. During closed door consideration of the measure, Senate leadership chose to bow to special interest groups despite the significant support COOL experiences from the majority of consumers and producers. While I was pleased to see the Senate version of the fiscal year 2006 bill that we reported out of committee contained $3.111 million for an audit-based compliance program for COOL implementation, the United States Department of Agriculture, USDA, Agricultural Marketing Service, AMS, will need substantive funding for the implementation of the full program. While the money funds an audit-based compliance program exclusively for fish and shellfish, additional dollars are needed for the inclusion of all covered commodities.

Mandatory COOL for fish and shellfish was implemented on April 4, 2005. USDA instituted a six month phase-in period to ensure adequate time for compliance, and the Department promulgated an interim final rule on September 30, 2004. Given this process, I see no reason why the Department should not proceed with the promulgation of the interim final rule for all covered commodities at the earliest possible time. If the implementation date is moved to January 30, 2006, then producers and consumers will at least see benefits under the program by late summer of 2006. Producers and consumers have waited long enough for program implementation, and it is high time USDA move forward with the implementation of this crucial program.

Mr. FEINGOLD. Mr. President, I am proud to join the chairman and the ranking member of the Senate Judiciary Committee in cosponsoring the Personal Data Privacy and Security Act of 2005. This bill is a much-needed solution to the daunting problem of ensuring the privacy and the security of our personal data, which has become such a precious commodity.

As we enter the 21st century, several forces are converging to make our personal information more valuable—and vulnerable—than ever. The world is going digital, and so is our personal data. In this day and age, almost everything we do results in a third party creating a digital record about us—digital records that we may not even realize exist. We seek the convenience of opening bank accounts and making major purchases over the Internet, often without ever speaking to another person face to face or even over the telephone, making identity theft easier and more lucrative. Businesses, nonprofits and even political parties are personalizing their messages, products and services to a degree we've never seen before, and they are willing to invest significant amounts of money in collecting personal information about potential customers or donors. And we are living in an age where identity-based screening and security programs can be vitally important, resulting in more information being collected about individuals in an attempt to identify them accurately.

As a result, personal information has become a hot commodity that is bought, sold, and—as so often happens when something becomes valuable—stolen.

We are at a crossroads. We all know about the security breaches that have been on the front pages of newspapers all over the country for the past 6 months. They have placed the identities of hundreds of thousands of Americans at risk.

But this is about much more than just information security. Until California law required ChoicePoint to notify individuals that their information was compromised and they might be vulnerable to identity theft, many Americans had never heard of this company. As news stories focused on the data broker business, many Americans were surprised to discover that companies are creating digital dossiers about them that contain massive amounts of information, and that these companies sell that information to commercial and government entities. The revelations about these security breaches highlighted the fact that Americans need a better understanding of what happens to their information in a digital world—and what kind of consequences they can face as a result.

When I am back home in Wisconsin, I hear from people who do not understand why companies have the right to sell their sensitive personal information. I hear from people who are shocked to discover that personal information about them is available for free on the Internet.

There is no question that data aggregators facilitate societal benefits, allowing consumers to obtain instant credit and personalized services, and police officers to locate suspects. But these companies also gather a great deal of potentially sensitive information about individuals, and in many instances they go largely unregulated.

Too many of my constituents feel they have lost control over their own information. Congress must return some power to individual Americans so that we can all better understand and manage what happens to our own personal data.

The Personal Data Privacy and Security Act takes a comprehensive approach to the privacy and security problems we face. It gives consumers back some control over their own information. The bill requires data brokers to allow consumers to access their own information, and to investigate when consumers tell them that corrections are necessary. And it requires companies to give notice to affected consumers and to law enforcement if there is a serious security breach, so that individuals know their identity may be at risk and can take steps to protect themselves.

In addition, the bill increases penalties for those who steal our identities. It provides grants to State and local law enforcement to help them combat data fraud and related crimes. It requires companies that buy and sell information to have appropriate data security systems in place. It provides protection to Social Security numbers by prohibiting the sale, purchase or display of Social Security numbers, with certain exceptions, and preventing companies from requiring customers to provide their Social Security numbers in order to purchase goods or services. These protections will help safeguard against future privacy violations and security breaches in the commercial data industry. But that is not all this bill accomplishes.

The bill also contains some critically important privacy and security provisions to govern the Government's use of commercial data. This is an aspect of the data broker business that has not yet gotten as much attention in the wake of the recent security breaches. The information gathered by these companies is not just sold to individuals and businesses; Government agencies of all stripes also buy or subscribe to information from commercial sources. The most recent example was the discovery that the Pentagon has a contract with a marketing firm to analyze commercial and other data about high school and college students.

While I believe the Government should be able to access commercial databases in appropriate circumstances, there are few existing rules or guidelines to ensure this information is used responsibly. Nor are there restrictions on the use of commercial data for powerful, intrusive data mining programs, an issue I have been particularly concerned about. The Privacy Act, which governs when Government agencies themselves are collecting data, does not apply because the information is held outside the Government and is not gathered solely at Government direction.

As a result, there is a great deal we do not know about Government use of commercial data, even in clearly appropriate circumstances such as when the agency's goal is simply to locate an individual already suspected of a crime.

We don't know under what circumstances Government employees can obtain access to these databases or for what purposes. We don't know how Government agencies evaluate the accuracy of the databases to which they subscribe, or how the accuracy level affects government use of the data. We don't know how employees are monitored to ensure they do not abuse their access to these databases, or how those who misuse the information are punished. And we don't know how Government agencies, particularly those engaged in sensitive national security investigations, ensure that the data brokers cannot keep records of who the Government is investigating, records which themselves could create a huge security risk in light of the vulnerabilities that have come to the forefront in recent months.

That is why I am so pleased that this bill includes provisions to address the Government's use of commercial data. A comprehensive approach to data privacy and security would be incomplete without taking on this piece of the puzzle. The bill recognizes there are many legitimate reasons for Government agencies to obtain commercially available data, but that they need to be subject to privacy and security protections. It takes a commonsense approach, pushing Government agencies to take basic steps to ensure that individuals' personal information is secure and only used for legitimate purposes, and that the commercial information the Government is paying for and relying on is accurate and complete.

Specifically, the bill would require that Federal agencies that subscribe to commercial data adopt standards governing its use. These standards would reflect long-standing basic privacy principles. The bill would ensure that Government agencies consider and determine which personnel will be permitted to access the information and under what circumstances; develop retention policies for this personal data and get rid of data they no longer need, minimizing the opportunity for abuse or theft; rely only on accurate and complete data, and penalize vendors who knowingly provide inaccurate information to the Federal Government; provide individuals who suffer adverse consequences as a result of the agency's reliance on commercial data with a redress mechanism; and establish enforcement mechanisms for those privacy policies.

The bill also extends to other screening programs the existing protections that already are in place to govern the Transportation Security Administration's possible use of commercial data for its identity-based airline passenger screening program, Secure Flight. If the Federal Government is going to rely on commercial data to screen Americans and decide whether to permit them to travel by air or engage in other common activities, it should do so only subject to explicit congressional authorization, as this bill provides. In addition, agencies should have to provide a redress process for those wrongly affected, and should have to operate under rules that govern the access, use, disclosure, accuracy and retention of that data.

The bill also directs the General Services Administration to review Government contracts for commercial data to make sure that vendors have appropriate security programs in place, and that they do not provide information to the Government that they know to be inaccurate. And it requires agencies to audit the information security practices of their vendors.

These are basic good Government measures. They guarantee that the Federal Government is not wasting money on inaccurate data, and that vendors are undertaking the security programs that they have promised and for which the Government is paying.

We live in a new digital world. The law may never fully keep up with technology, but we must make every effort we can. I am proud to be involved in this comprehensive, reasoned approach to privacy and security. I congratulate Chairman SPECTER and Ranking Member LEAHY for their excellent work on this bill. This bill is important and it deserves very serious consideration by the Senate.

By Mr. SPECTER (for himself and Mr. LEAHY):

S. 1332. A bill to prevent and mitigate identity theft; to ensure privacy; and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information; read the first time.

Mr. SPECTER. Mr. President, I rise today to introduce S. 1332, the Personal Data Privacy and Security Act of 2005.

Not too long ago, our personal information—our Social Security numbers, our date of birth, our mothers' maiden name, where we live-all remained relatively private. Where we live, and what we paid for our house, and whether we had a mortgage might have been publicly available, but finding that information out would require a trip to

the local recorders office. Our privacy was preserved by the sheer difficulty of obtaining the information. This privacy—the ability to be left alone—has been a cherished value throughout American history.

As our day-to-day transactions have become electronic, more and more of our personal data has been stored, transmitted and accessed electronically. Almost all of us have benefited from this change. Because our personal information is available electronically, we can purchase goods and services over the phone or on the internet. We can obtain a mortgage or rent an apartment in a matter of hours. We can apply for a credit card while we wait at the store and purchase things on-line. The availability of such information also helps law enforcement agencies conduct investigations and catch criminals. The information has also been used to do good. In one instance, Associated Press journalists matched Social Security numbers obtained from data brokers to Mississippi prison data exposing eight school teachers who failed to report that they had been convicted of sex offenses or drug crimes.

However, as Justice Warren prophetically wrote in the 1963 case, Lopez v. United States—a case balancing the privacy interests of an individual with the law enforcement needs of the government—''The fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual.'' In electronic form, our personal information is both more valuable and more vulnerable. As we have all witnessed in recent months, electronic data is more vulnerable because it can be accessed from afar and can be stolen in a split second. The problem first became apparent when data brokers, companies that buy and sell our personal data, announced that they had experienced large-scale breaches involving the personal data of hundreds of thousands of Americans. In February, ChoicePoint, one of the Nation's largest collectors of consumer information, notified over 145,000 Americans of a system security breach. In March, LexisNexis announced that unauthorized persons posing as legitimate customers obtained personal the personal data of over 300,000 Americans.

It soon became apparent that the problem extended beyond data brokers. In April, Carnegie Mellon University notified 19,000 students, alumni, faculty and staff that their personal data may have been compromised. In May, a data storage company lost information on 600,000 current and former employees of Time Warner. In recent days, MasterCard announced 40 million credit card numbers belonging to U.S. consumers were accessed by a computer hacker—the largest breach yet.

Even government agencies have not been immune. Personal data including Social Security numbers on nearly 6,000 current and former Federal Deposit Insurance Corporation employees was stolen early last year, some of which has been used for fraudulent purposes.

Electronic personal data is more valuable because identity thieves can steal large volumes and use it before anyone knows. For the last 5 years, Identity Theft has topped the FTC's list of consumer complaints. From 2002 to 2004, the number of complaints rose 52 percent, to 246,570. Put another way, that's once every 2 minutes. But this is only the tip of the iceberg. Not all consumers report identity theft to the FTC. Not all victims report identity theft to their local police. Sixty percent of those who did file a report with the FTC did not call their local police department. It stands to reason that many did not call the FTC.

A recent study by the Better Business Bureau concluded that 9.3 million Americans were victims of identity fraud in 2004, and that each victim lost approximately $5,800. Ultimately, nearly 20 percent Americans will become victims of identity theft. Worse, according to the study, it took victims an average of 28 hours on the phone with creditors and credit bureaus to clear their names. I use the term ''clear'' loosely, because in many cases the damage caused by identity theft is irreversible. Victims will have fraud alerts on their credit reports for years to come, making it more difficult to open new accounts or make major purchases. Some will be erroneously contacted by collection agencies.

Individuals whose personal information is not stolen also suffer. Businesses lose nearly $50 billion a year from identity thieves posing as customers. These losses translate into increased prices for every consumer.

In some cases, the availability of electronic personal data can lead to tragedy. In 1999, a former high school classmate of Amy Lynn Boyer obtained her former work address and social security number from an on-line data broker. By calling her home and posing as the former employer, he convinced Amy's mom to give him Amy's work address. He then drove to Boyer's workplace and fatally shot her.

In an effort to protect the privacy and security of our electronic personal information, and prevent future tragedies, small and large, my colleague Senator LEAHY and I are introducing the Personal Data Privacy and Security Act of 2005. First, this legislation goes after identity thieves by increasing penalties for crimes involving electronic personal data. For example, it increases penalties for computer fraud when such fraud involves personal data. It also goes after those who intentionally expose Americans to identity theft by punishing those who intentionally conceal a security breach that involves personal data.

The bill also empowers Americans to look after the privacy of their own data. The bill will allow individuals to obtain access to any personal information held by data brokers. For individuals who believe their information is wrong, data brokers must provide them with guidance on how to correct their information.

The legislation also puts the burden those that store, transmit and access electronic personal data. It will require the companies, government agencies, universities that keep significant amounts of personal data to assess the vulnerability of their systems and to adopt policies that will address those vulnerabilities. Some entities will choose to encrypt the personal data that they store and transmit. Others will pick a means more appropriate their size and the sensitivity of their data.

Of course, these provisions do not apply to data held by health care providers and financial institutions that is already regulated by other federal laws. This legislation fills in gaps left by other federal laws. It has become clear that many entities other than health care providers and financial institutions have large amounts of personal information. This legislation would require such entities to adequately protect their electronic data.

Such measures will not always be enough. As I've already noted, the nature of electronic data makes it vulnerable even when those who hold it take reasonable steps to protect it. Currently, no federal law requires those who maintain our sensitive personal data to notify affected individuals when such data is lost or exposed. This legislation would require those who maintained such data to notify affected individuals as well as law enforcement. As everyone knows, knowledge is power. Once individuals learn that their personal information is exposed, they can take steps to protect themselves. And, the company, school or agency that experienced the breach must help. They must provide individuals whose data was lost with a monthly credit report and they must provide information on the identity theft victim assistance available to them. For large breaches, the media must be notified. Media reports over the past few months have made Americans far more aware of the problem of security breaches. Hopefully, we can continue to raise awareness by requiring data holders to continue the practice of making public announcements regarding large breaches. Notice will also give law enforcement a head start in the effort to prevent harm to individuals as a result of a breach.

One of the most critical pieces of information that can be lost is one's Social Security number. We can all think of instances when we've been asked for our Social Security number to verify our identities—utilities, doctors, schools—I could go on. In itself, this is not harmful. Problems arise however, when the Social Security number gets passed along to others without the person's knowledge or permission. The legislation would prohibit companies from buying, selling or displaying a Social Security number without consent

from the individual whose number it is. The bill also would prevent companies from requiring individuals to give their Social Security number in order to obtain goods or services. Finally, it would bar government agencies from posting public records that contain Social Security numbers on the internet. This legislation would not prevent the use of Social Security numbers altogether. We recognize that would not be practical. It would, however, protect the value of Social Security numbers by preventing their proliferation.

Finally, this legislation will protect the privacy of all Americans by providing a check on the government's use of databases maintained by data brokers. As I've already noted, federal law enforcement uses electronic personal data maintained by data brokers to track criminals and criminal activity. Correctly used, these databases can be very useful tools in the fight against crime. However, there should be some check on their use. In addition, the legislation aims at making sure the government's use of such data is secure. It will require audits to ensure that data brokers are keeping law enforcement inquiries private.

This bill represents a comprehensive effort to protect the privacy and security of electronic personal data. Our lives have all been made easier because our personal information is readily available to those who have a legitimate need for it. This legislation aims to keep such information out of the hands of those who have no legitimate need for it. I urge my colleagues to join me in supporting this important legislation. I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the bill was ordered to be printed in the RECORD, as follows:

S. 1332

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Personal Data Privacy and Security Act of 2005''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. FINDINGS.

Congress finds that—

(1) databases of personal identifiable information are increasingly prime targets of hackers, identity thieves, rogue employees, and other criminals, including organized and sophisticated criminal operations;

(2) identity theft is a serious threat to the nation's economic stability, homeland security, the development of e-commerce, and the privacy rights of Americans;

(3) over 9,300,000 individuals were victims of identity theft in America last year;

(4) security breaches are a serious threat to consumer confidence, homeland security, e-commerce, and economic stability;

(5) it is important for business entities that own, use, or license personally identifiable information to adopt reasonable procedures to ensure the security, privacy, and confidentially of that personally identifiable information;

(6) individuals whose personal information has been compromised or who have been victims of identity theft should receive the necessary information and assistance to mitigate their damages and to restore the integrity of their personal information and identities;

(7) data brokers have assumed a significant role in providing identification, authentication, and screening services, and related data collection and analyses for commercial, nonprofit, and government operations;

(8) data misuse and use of inaccurate data have the potential to cause serious or irreparable harm to an individual's livelihood, privacy, and liberty and undermine efficient and effective business and government operations;

(9) there is a need to insure that data brokers conduct their operations in a manner that prioritizes fairness, transparency, accuracy, and respect for the privacy of consumers;

(10) government access to commercial data can potentially improve safety, law enforcement, and national security; and

(11) because government misuse of commercial data endangers privacy, security, and liberty, there is a need for Congress to exercise oversight over government use of commercial data.

SEC. 3. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''agency'' has the same meaning given such term in section 551 of title 5, United States Code.

(2) AFFILIATE.—The term ''affiliate'' means persons related by common ownership or affiliated by corporate control.

(3) BUSINESS ENTITY.—The term ''business entity'' means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, venture established to make a profit, or nonprofit, and any contractor, subcontractor, affiliate, or licensee thereof engaged in interstate commerce.

(4) IDENTITY THEFT.—The term ''identity theft'' means a violation of section 1028 of title 18, United States Code, or any other similar provision of applicable State law.

(5) DATA BROKER.—The term ''data broker'' means a business entity which for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of collecting, transmitting, or otherwise providing personally identifiable information on a nationwide basis on more than 5,000 individuals who are not the customers or employees of the business entity or affiliate.

(6) DATA FURNISHER.—The term ''data furnisher'' means any agency, governmental entity, organization, corporation, trust, partnership, sole proprietorship, unincorporated association, venture established to make a profit, or nonprofit, and any contractor, subcontractor, affiliate, or licensee thereof, that serves as a source of information for a data broker.

(7) PERSONAL ELECTRONIC RECORD.—The term ''personal electronic record'' means the

compilation of personally identifiable information of an individual (including information associated with that personally identifiable information) in a database, networked or integrated databases, or other data system.

(8) PERSONALLY IDENTIFIABLE INFORMATION.—The term ''personally identifiable information'' means any information, or compilation of information, in electronic or digital form serving as a means of identification, as defined by section 1028(d)(7) of title 18, United State Code.

(9) PUBLIC RECORD.—The term ''public record'' means any item, collection, or grouping of information about an individual that is maintained by an agency, including—

(A) education, financial transactions, medical history, and criminal or employment history containing the name of an individual; and

(B) the identifying number, symbol, or other identifying particular assigned to an individual, such as—

(i) a fingerprint;

(ii) a voice print; or

(iii) a photograph.

(10) SECURITY BREACH.—

(A) IN GENERAL.—The term ''security breach'' means compromise of the security, confidentiality, or integrity of computerized data through misrepresentation or actions that result in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to sensitive personally identifiable information.

(B) EXCLUSION.—The term ''security breach'' does not include a good faith acquisition of sensitive personally identifiable information if the sensitive personally identifiable information is not subject to further unauthorized disclosure.

(11) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''sensitive personally identifiable information'' means any name or number used in conjunction with any other information to identify a specific individual, including any—

(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as—

(i) a fingerprint;

(ii) a voice print;

(iii) a retina or iris image; or

(iv) any other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device (as defined in section 1029(e) of title 18, United States Code).

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

SEC. 101. FRAUD AND RELATED CRIMINAL ACTIVITY IN CONNECTION WITH UNAUTHORIZED ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION.

Section 1030(a)(2) of title 18, United States Code, is amended—

(1) in subparagraph (B), by striking ''or'' after the semicolon;

(2) in subparagraph (C), by inserting ''or'' after the semicolon; and

(3) by adding at the end the following:

''(D) information contained in the databases or systems of a data broker, or in other personal electronic records, as such terms are defined in section 3 of the Personal Data Privacy and Security Act of 2005;''.

SEC. 102. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION WITH UNAUTHORIZED ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION.

Section 1961(1) of title 18, United States Code, is amended by inserting ''section 1030(a)(2)(D)(relating to fraud and related activity in connection with unauthorized access to personally identifiable information,'' before ''section 1084''.

SEC. 103. CONCEALMENT OF SECURITY BREACHES INVOLVING PERSONALLY IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''§ 1039. Concealment of security breaches involving personally identifiable information

''Whoever, having knowledge of a security breach requiring notice to individuals under title IV of the Personal Data Privacy and Security Act of 2005, intentionally and willfully conceals the fact of, or information related to, such security breach, shall be fined under this title or imprisoned not more than 5 years, or both.''.

(b) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''1039. Concealment of security breaches involving personally identifiable information.''.

SEC. 104. AGGRAVATED FRAUD IN CONNECTION WITH COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding after section 1030 the following:

''§ 1030A. Aggravated fraud in connection with computers

''(a) IN GENERAL.—Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly obtains, accesses, or transmits, without lawful authority, a means of identification of another person may, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of up to 2 years.

''(b) CONSECUTIVE SENTENCES.—Notwithstanding any other provision of law, should a court in its discretion impose an additional sentence under subsection (a)—

''(1) no term of imprisonment imposed on a person under this section shall run concurrently, except as provided in paragraph (3), with any other term of imprisonment imposed on such person under any other provision of law, including any term of imprisonment imposed for the felony during which the means of identifications was obtained, accessed, or transmitted;

''(2) in determining any term of imprisonment to be imposed for the felony during which the means of identification was obtained, accessed, or transmitted, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(3) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section.

''(c) DEFINITION.—For purposes of this section, the term 'felony violation enumerated in subsection (c)' means any offense that is a felony violation of paragraphs (2) through (7) of section 1030(a).''.

(b) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following new item:

''1030A. Aggravated fraud in connection with computers.''.

SEC. 105. REVIEW AND AMENDMENT OF FEDERAL SENTENCING GUIDELINES RELATED TO FRAUDULENT ACCESS TO OR MISUSE OF DIGITIZED OR ELECTRONIC PERSONALLY IDENTIFIABLE INFORMATION.

(a) REVIEW AND AMENDMENT.—Not later than 180 days after the date of enactment of this Act, the United States Sentencing Commission, pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, shall review and, if appropriate, amend the Federal sentencing guidelines (including its policy statements) applicable to persons convicted of using fraud to access, or misuse of, digitized or electronic personally identifiable information, including identity theft or any offense under—

(1) sections 1028, 1028A, 1030, 1030A, 2511, and 2701 of title 18, United States Code; or

(2) any other relevant provision.

(b) REQUIREMENTS.—In carrying out the requirements of this section, the United States Sentencing Commission shall—

(1) ensure that the Federal sentencing guidelines (including its policy statements) reflect—

(A) the serious nature of the offenses and penalties referred to in this Act;

(B) the growing incidences of theft and misuse of digitized or electronic personally identifiable information, including identity theft; and

(C) the need to deter, prevent, and punish such offenses;

(2) consider the extent to which the Federal sentencing guidelines (including its policy statements) adequately address violations of the sections amended by this Act to—

(A) sufficiently deter and punish such offenses; and

(B) adequately reflect the enhanced penalties established under this Act;

(3) maintain reasonable consistency with other relevant directives and sentencing guidelines;

(4) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(5) consider whether to provide a sentencing enhancement for those convicted of the offenses described in subsection (a), if the conduct involves—

(A) the online sale of fraudulently obtained or stolen personally identifiable information;

(B) the sale of fraudulently obtained or stolen personally identifiable information to an individual who is engaged in terrorist activity or aiding other individuals engaged in terrorist activity; or

(C) the sale of fraudulently obtained or stolen personally identifiable information to finance terrorist activity or other criminal activities;

(6) make any necessary conforming changes to the Federal sentencing guidelines to ensure that such guidelines (including its policy statements) as described in subsection (a) are sufficiently stringent to deter, and adequately reflect crimes related to fraudulent access to, or misuse of, personally identifiable information; and

(7) ensure that the Federal sentencing guidelines adequately meet the purposes of sentencing under section 3553(a)(2) of title 18, United States Code.

(c) EMERGENCY AUTHORITY TO SENTENCING COMMISSION.—The United States Sentencing Commission may, as soon as practicable, promulgate amendments under this section in accordance with procedures established in section 21(a) of the Sentencing Act of 1987 (28

U.S.C. 994 note) as though the authority under that Act had not expired.

TITLE II—ASSISTANCE FOR STATE AND LOCAL LAW ENFORCEMENT COMBATING CRIMES RELATED TO FRAUDULENT, UNAUTHORIZED, OR OTHER CRIMINAL USE OF PERSONALLY IDENTIFIABLE INFORMATION

SEC. 201. GRANTS FOR STATE AND LOCAL ENFORCEMENT.

(a) IN GENERAL.—Subject to the availability of amounts provided in advance in appropriations Acts, the Assistant Attorney General for the Office of Justice Programs of the Department of Justice may award a grant to a State to establish and develop programs to increase and enhance enforcement against crimes related to fraudulent, unauthorized, or other criminal use of personally identifiable information.

(b) APPLICATION.—A State seeking a grant under subsection (a) shall submit an application to the Assistant Attorney General for the Office of Justice Programs of the Department of Justice at such time, in such manner, and containing such information as the Assistant Attorney General may require.

(c) USE OF GRANT AMOUNTS.—A grant awarded to a State under subsection (a) shall be used by a State, in conjunction with units of local government within that State, State and local courts, other States, or combinations thereof, to establish and develop programs to—

(1) assist State and local law enforcement agencies in enforcing State and local criminal laws relating to crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information;

(2) assist State and local law enforcement agencies in educating the public to prevent and identify crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information;

(3) educate and train State and local law enforcement officers and prosecutors to conduct investigations and forensic analyses of evidence and prosecutions of crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information;

(4) assist State and local law enforcement officers and prosecutors in acquiring computer and other equipment to conduct investigations and forensic analysis of evidence of crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information; and

(5) facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information with State and local law enforcement officers and prosecutors, including the use of multi-jurisdictional task forces.

(d) ASSURANCES AND ELIGIBILITY.—To be eligible to receive a grant under subsection (a), a State shall provide assurances to the Attorney General that the State—

(1) has in effect laws that penalize crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information, such as penal laws prohibiting—

(A) fraudulent schemes executed to obtain personally identifiable information;

(B) schemes executed to sell or use fraudulently obtained personally identifiable information; and

(C) online sales of personally identifiable information obtained fraudulently or by other illegal means;

(2) will provide an assessment of the resource needs of the State and units of local government within that State, including criminal justice resources being devoted to the investigation and enforcement of laws related to crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information; and

(3) will develop a plan for coordinating the programs funded under this section with other federally funded technical assistant and training programs, including directly funded local programs such as the Local Law Enforcement Block Grant program (described under the heading ''Violent Crime Reduction Programs, State and Local Law Enforcement Assistance'' of the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 1998 (Public Law 105–119)).

(e) MATCHING FUNDS.—The Federal share of a grant received under this section may not exceed 90 percent of the total cost of a program or proposal funded under this section unless the Attorney General waives, wholly or in part, the requirements of this subsection.

SEC. 202. AUTHORIZATION OF APPROPRIATIONS.

(a) IN GENERAL.—There is authorized to be appropriated to carry out this title $25,000,000 for each of fiscal years 2006 through 2009.

(b) LIMITATIONS.—Of the amount made available to carry out this title in any fiscal year not more than 3 percent may be used by the Attorney General for salaries and administrative expenses.

(c) MINIMUM AMOUNT.—Unless all eligible applications submitted by a State or units of local government within a State for a grant under this title have been funded, the State, together with grantees within the State (other than Indian tribes), shall be allocated in each fiscal year under this title not less than 0.75 percent of the total amount appropriated in the fiscal year for grants pursuant to this title, except that the United States Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands each shall be allocated 0.25 percent.

(d) GRANTS TO INDIAN TRIBES.—Notwithstanding any other provision of this title, the Attorney General may use amounts made available under this title to make grants to Indian tribes for use in accordance with this title.

TITLE III—DATA BROKERS

SEC. 301. TRANSPARENCY AND ACCURACY OF DATA COLLECTION.

(a) IN GENERAL.—Data brokers engaging in interstate commerce are subject to the requirements of this title for any offered product or service offered to third parties that allows access, use, compilation, distribution, processing, analyzing, or evaluating personally identifiable information, unless that product or service is currently subject to similar protections under subsections (b) and (g) of this section, the Fair Credit Reporting Act (Public Law 91–508), or the Gramm-Leach Bliley Act (Public Law 106–102), and implementing regulations.

(b) DISCLOSURES TO INDIVIDUALS.—

(1) IN GENERAL.—A data broker shall, upon the request of an individual, clearly and accurately disclose to such individual for a reasonable fee all personal electronic records pertaining to that individual maintained for disclosure to third parties in the databases or systems of the data broker at the time of the request.

(2) INFORMATION ON HOW TO CORRECT INACCURACIES.—The disclosures required under paragraph (1) shall also include guidance to individuals on the processes and procedures for demonstrating and correcting any inaccuracies.

(c) CREATION OF AN ACCURACY RESOLUTION PROCESS.—A data broker shall develop and publish on its website timely and fair processes and procedures for responding to claims of inaccuracies, including procedures for correcting inaccurate information in the personal electronic records it maintains on individuals.

(d) ACCURACY RESOLUTION PROCESS.—

(1) PUBLIC RECORD INFORMATION.—

(A) IN GENERAL.—If an individual notifies a data broker of a dispute as to the completeness or accuracy of information, and the data broker determines that such information is derived from a public record source, the data broker shall determine within 30 days whether the information in its system accurately and completely records the information offered by the public record source.

(B) DATA BROKER ACTIONS.—If a data broker determines under subparagraph (A) that the information in its systems—

(i) does not accurately and completely record the information offered by a public record source, the data broker shall correct any inaccuracies or incompleteness, and provide to such individual written notice of such changes; and

(ii) does accurately and completely record the information offered by a public record source, the data broker shall—

(I) provide such individual with the name, address, and telephone contact information of the public record source; and

(II) notify such individual of the right to add to the personal electronic record of the individual maintained by the data broker a statement disputing the accuracy or completeness of the information for a period of 90 days under subsection (e).

(2) INVESTIGATION OF DISPUTED NON-PUBLIC RECORD INFORMATION.—If the completeness or accuracy of any non-public record information disclosed to an individual under subsection (b) is disputed by the individual and such individual notifies the data broker directly of such dispute, the data broker shall, before the end of the 30-day period beginning on the date on which the data broker receives the notice of the dispute—

(A) investigate free of charge and record the current status of the disputed information; or

(B) delete the item from the individuals data file in accordance with paragraph (8).

(3) EXTENSION OF PERIOD TO INVESTIGATE.—Except as provided in paragraph (4), the 30-day period described in paragraph (1) may be extended for not more than 15 additional days if a data broker receives information from the individual during that 30-day period that is relevant to the investigation.

(4) LIMITATIONS ON EXTENSION OF PERIOD TO INVESTIGATE.—Paragraph (3) shall not apply to any investigation in which, during the 30-day period described in paragraph (1), the information that is the subject of the investigation is found to be inaccurate or incomplete or a data broker determines that the information cannot be verified.

(5) NOTICE IDENTIFYING THE DATA FURNISHER.—If the completeness or accuracy of any information disclosed to an individual under subsection (b) is disputed by the individual, a data broker shall provide upon the request of the individual, the name, business address, and telephone contact information of any data furnisher who provided an item of information in dispute.

(6) DETERMINATION THAT DISPUTE IS FRIVOLOUS OR IRRELEVANT.—

(A) IN GENERAL.—Notwithstanding paragraphs (1) through (4), a data broker may decline to investigate or terminate an investigation of information disputed by an individual under those paragraphs if the data broker reasonably determines that the dispute by the individual is frivolous or irrelevant, including by reason of a failure by the individual to provide sufficient information to investigate the disputed information.

(B) NOTICE.—Not later than 5 business days after making any determination in accordance with subparagraph (A) that a dispute is frivolous or irrelevant, a data broker shall notify the individual of such determination by mail, or if authorized by the individual, by any other means available to the data broker.

(C) CONTENTS OF NOTICE.—A notice under subparagraph (B) shall include—

(i) the reasons for the determination under subparagraph (A); and

(ii) identification of any information required to investigate the disputed information, which may consist of a standardized form describing the general nature of such information.

(7) CONSIDERATION OF INDIVIDUAL INFORMATION.—In conducting any investigation with respect to disputed information in the personal electronic record of any individual, a data broker shall review and consider all relevant information submitted by the individual in the period described in paragraph (2) with respect to such disputed information.

(8) TREATMENT OF INACCURATE OR UNVERIFIABLE INFORMATION.—

(A) IN GENERAL.—If, after any review of public record information under paragraph (1) or any investigation of any information disputed by an individual under paragraphs (2) through (4), an item of information is found to be inaccurate or incomplete or cannot be verified, a data broker shall promptly delete that item of information from the individual's personal electronic record or modify that item of information, as appropriate, based on the results of the investigation.

(B) NOTICE TO INDIVIDUALS OF REINSERTION OF PREVIOUSLY DELETED INFORMATION.—If any information that has been deleted from an individual's personal electronic record pursuant to subparagraph (A) is reinserted in the personal electronic record of the individual, a data broker shall, not later than 5 days after reinsertion, notify the individual of the reinsertion and identify any data furnisher not previously disclosed in writing, or if authorized by the individual for that purpose, by any other means available to the data broker, unless such notification has been previously given under this subsection.

(C) NOTICE OF RESULTS OF INVESTIGATION OF DISPUTED NON-PUBLIC RECORD.—

(i) IN GENERAL.—Not later than 5 business days after the completion of an investigation under paragraph (2), a data broker shall provide written notice to an individual of the results of the investigation, by mail or, if authorized by the individual for that purpose, by other means available to the data broker.

(ii) ADDITIONAL REQUIREMENT.—Before the expiration of the 5-day period, as part of, or in addition to such notice, a data broker shall, in writing, provide to an individual—

(I) a statement that the investigation is completed;

(II) a report that is based upon the personal electronic record of such individual as that personal electronic record is revised as a result of the investigation;

(III) a notice that, if requested by the individual, a description of the procedures used to determine the accuracy and completeness of the information shall be provided to the individual by the data broker, including the business name, address, and telephone number of any data furnisher of information contacted in connection with such information; and

(IV) a notice that the individual has the right to request notifications under subsection (g).

(D) DESCRIPTION OF INVESTIGATION PROCEDURES.—Not later than 15 days after receiving a request from an individual for a description referred to in subparagraph (C)(ii)(III), a data broker shall provide to the individual such a description.

(E) EXPEDITED DISPUTE RESOLUTION.—If by no later than 3 business days after the date on which a data broker receives notice of a dispute from an individual of information in the personal electronic record of such individual in accordance with paragraph (2), a data broker resolves such dispute in accordance with subparagraph (A) by the deletion of the disputed information, then the data broker shall not be required to comply with subsections (e) and (f) with respect to that dispute if the data broker provides—

(i) to the individual, by telephone, prompt notice of the deletion; and

(ii) to the individual a right to request that the data broker furnish notifications under subsection (g).

(e) STATEMENT OF DISPUTE.—

(1) IN GENERAL.—If the completeness or accuracy of any information disclosed to an individual under subsection (b) is disputed, an individual may file a brief statement setting forth the nature of the dispute.

(2) CONTENTS OF STATEMENT.—A data broker may limit the statements made pursuant to paragraph (1) to not more than 100 words if it provides an individual with assistance in writing a clear summary of the dispute or until the dispute is resolved, whichever is earlier.

(f) NOTIFICATION OF DISPUTE IN SUBSEQUENT REPORTS.—Whenever a statement of a dispute is filed under subsection (e), unless there is a reasonable grounds to believe that it is frivolous or irrelevant, a data broker shall, in any subsequent report, product, or service containing the information in question, clearly note that it is disputed by an individual and provide either the statement of such individual or a clear and accurate codification or summary thereof for a period of 90 days after the data broker first posts the statement of dispute.

(g) NOTIFICATION OF DELETION OF DISPUTED INFORMATION.—Following any deletion of information which is found to be inaccurate or whose accuracy can no longer be verified, a data broker shall, at the request of an individual, furnish notification that the item has been deleted or the statement, codification, or summary pursuant to subsection (e) or (f) to any user or customer of the products or services of the data broker who has within 90 days received a report with the deleted or disputed information or has electronically accessed the deleted or disputed information.

SEC. 302. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) PENALTIES.—Any data broker that violates the provisions of section 301 shall be subject to civil penalties of not more than $1,000 per violation per day, with a maximum of $15,000 per day, while such violations persist.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A data broker that intentionally or willfully violates the provisions of section 301 shall be subject to additional penalties in the amount of $1,000 per violation per day, with a maximum of an additional $15,000 per day, while such violations persist.

(3) EQUITABLE RELIEF.—A data broker engaged in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this subsection are cumulative and shall not affect any other rights and remedies available under law.

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—Whenever it appears that a data broker to which this title applies has engaged, is engaged, or is about to engage, in any act or practice constituting a violation of this title, the Attorney General may bring a civil action in an appropriate district court of the United States to—

(A) enjoin such act or practice;

(B) enforce compliance with this title;

(C) obtain damages—

(i) in the sum of actual damages, restitution, and other compensation on behalf of the affected residents of a State; and

(ii) punitive damages, if the violation is willful or intentional; and

(D) obtain such other relief as the court determines to be appropriate.

(2) OTHER INJUNCTIVE RELIEF.—Upon a proper showing in the action under paragraph (1), the court shall grant a permanent injunction or a temporary restraining order without bond.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by an act or practice that violates this title, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this title;

(C) obtain—

(i) damages in the sum of actual damages, restitution, or other compensation on behalf of affected residents of the State; and

(ii) punitive damages, if the violation is willful or intentional; or

(D) obtain such other legal and equitable relief as the court may consider to be appropriate.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Attorney General—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Attorney General as soon after the filing of the complaint as practicable.

(3) ATTORNEY GENERAL AUTHORITY.—Upon receiving notice under paragraph (2), the Attorney General shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation of this Act or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths and affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1931 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

SEC. 303. RELATION TO STATE LAWS.

(a) IN GENERAL.—Except as provided in subsection (b), this title does not annul, alter, affect, or exempt any person subject to the provisions of this title from complying with the laws of any State with respect to the access, use, compilation, distribution, processing, analysis, and evaluation of any personally identifiable information by data brokers, except to the extent that those laws are inconsistent with any provisions of this title, and then only to the extent of such inconsistency.

(b) EXCEPTIONS.—No requirement or prohibition may be imposed under the laws of any State with respect to any subject matter regulated under section 301, relating to individual access to, and correction of, personal electronic records.

SEC. 304. EFFECTIVE DATE.

This title shall take effect 180 days after the date of enactment of this Act.

TITLE IV—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—Data Privacy and Security Program

SEC. 401. PURPOSE AND APPLICABILITY OF DATA PRIVACY AND SECURITY PROGRAM.

(a) PURPOSE.—The purpose of this subtitle is to ensure standards for developing and implementing administrative, technical, and physical safeguards to protect the privacy, security, confidentiality, integrity, storage, and disposal of personally identifiable information.

(b) IN GENERAL.—A business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of personally identifiable information in electronic or digital form on 10,000 or more United States persons is subject to the requirements for a data privacy and security program under section 402 for protecting personally identifiable information.

(c) LIMITATIONS.—Notwithstanding any other obligation under this subtitle, this subtitle does not apply to—

(1) financial institutions subject to—

(A) the data security requirements and implementing regulations under the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.); and

(B) examinations for compliance with the requirements of this Act by 1 or more Federal functional regulators (as defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)); or

(2) ''covered entities'' subject to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including the data security requirements and implementing regulations of that Act.

SEC. 402. REQUIREMENTS FOR A PERSONAL DATA PRIVACY AND SECURITY PROGRAM.

(a) PERSONAL DATA PRIVACY AND SECURITY PROGRAM.—Unless otherwise limited under section 401(c), a business entity subject to this subtitle shall comply with the following safeguards to protect the privacy and security of personally identifiable information:

(1) SCOPE.—A business entity shall implement a comprehensive personal data privacy and security program, written in 1 or more readily accessible parts, that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the business entity and the nature and scope of its activities.

(2) DESIGN.—The personal data privacy and security program shall be designed to—

(A) ensure the privacy, security, and confidentiality of personal electronic records;

(B) protect against any anticipated vulnerabilities to the privacy, security, or integrity of personal electronic records; and

(C) protect against unauthorized access to use of personal electronic records that could result in substantial harm or inconvenience to any individual.

(3) RISK ASSESSMENT.—A business entity shall—

(A) identify reasonably foreseeable internal and external vulnerabilities that could result in unauthorized access, disclosure, use, or alteration of personally identifiable information or systems containing personally identifiable information;

(B) assess the likelihood of and potential damage from unauthorized access, disclosure, use, or alteration of personally identifiable information; and

(C) assess the sufficiency of its policies, technologies, and safeguards in place to control and minimize risks from unauthorized access, disclosure, use, or alteration of personally identifiable information.

(4) RISK MANAGEMENT AND CONTROL.—Each business entity shall—

(A) design its personal data privacy and security program to control the risks identified under paragraph (3); and

(B) adopt measures commensurate with the sensitivity of the data as well as the size, complexity, and scope of the activities of the business entity that—

(i) control access to systems and facilities containing personally identifiable information, including controls to authenticate and permit access only to authorized individuals;

(ii) detect actual and attempted fraudulent, unlawful, or unauthorized access, disclosure, use, or alteration of personally identifiable information, including by employees and other individuals otherwise authorized to have access; and

(iii) protect personally identifiable information during use, transmission, storage, and disposal by encryption or other reasonable means (including as directed for disposal of records under section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w) and the implementing regulations of such Act as set forth in section 682 of title 16, Code of Federal Regulations).

(5) ACCOUNTABILITY.—Each business entity required to establish a data security program under section 401 shall publish on its website or make otherwise available the terms of such program to the extent that such terms do not reveal information that compromise data security or privacy.

(b) TRAINING.—Each business entity subject to this subtitle shall take steps to ensure employee training and supervision for implementation of the data security program of the business entity.

(c) VULNERABILITY TESTING.—

(1) IN GENERAL.—Each business entity subject to this subtitle shall take steps to ensure regular testing of key controls, systems, and procedures of the personal data privacy and security program to detect, prevent, and respond to attacks or intrusions, or other system failures.

(2) FREQUENCY.—The frequency and nature of the tests required under paragraph (1) shall be determined by the risk assessment of the business entity under subsection (a)(3).

(d) RELATIONSHIP TO SERVICE PROVIDERS.—In the event a business entity subject to this subtitle engages service providers not subject to this subtitle, such business entity shall—

(1) exercise appropriate due diligence in selecting those service providers for responsibilities related to personally identifiable information, and take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the personally identifiable information at issue; and

(2) require those service providers by contract to implement and maintain appropriate measures designed to meet the objectives and requirements governing entities subject to this section, section 401, and subtitle B.

(e) PERIODIC ASSESSMENT AND PERSONAL DATA PRIVACY AND SECURITY MODERNIZATION.—Each business entity subject to this subtitle shall on a regular basis monitor, evaluate, and adjust, as appropriate its data privacy and security program in light of any relevant changes in—

(1) technology;

(2) the sensitivity of personally identifiable information;

(3) internal or external threats to personally identifiable information; and

(4) the changing business arrangements of the business entity, such as—

(A) mergers and acquisitions;

(B) alliances and joint ventures;

(C) outsourcing arrangements;

(D) bankruptcy; and

(E) changes to personally identifiable information systems.

(f) IMPLEMENTATION TIME LINE.—Not later than 1 year after the date of enactment of this Act, a business entity subject to the provisions of this subtitle shall implement a data privacy and security program pursuant to this subtitle.

SEC. 403. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—Any business entity that violates the provisions of sections 401 or 402 shall be subject to civil penalties of not more than $5,000 per violation per day, with a maximum of $35,000 per day, while such violations persist.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A business entity that intentionally or willfully violates the provisions of sections 401 or 402 shall be subject to additional penalties in the amount of $5,000 per violation per day, with a maximum of an additional $35,000 per day, while such violations persist.

(3) EQUITABLE RELIEF.—A business entity engaged in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are cumulative and shall not affect any other rights and remedies available under law

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—Whenever it appears that a business entity or agency to which this subtitle applies has engaged, is engaged, or is about to engage, in any act or practice constituting a violation of this subtitle, the Attorney General may bring a civil action in an appropriate district court of the United States to—

(A) enjoin such act or practice;

(B) enforce compliance with this subtitle; and

(C) obtain damages—

(i) in the sum of actual damages, restitution, and other compensation on behalf of the affected residents of a State; and

(ii) punitive damages, if the violation is willful or intentional; and

(D) obtain such other relief as the court determines to be appropriate.

(2) OTHER INJUNCTIVE RELIEF.—Upon a proper showing in the action under paragraph (1), the court shall grant a permanent injunction or a temporary restraining order without bond.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by an act or practice that violates this subtitle, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this subtitle;

(C) obtain—

(i) damages in the sum of actual damages, restitution, or other compensation on behalf of affected residents of the State; and

(ii) punitive damages, if the violation is willful or intentional; or

(D) obtain such other legal and equitable relief as the court may consider to be appropriate.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Attorney General—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Attorney General as soon after the filing of the complaint as practicable.

(3) ATTORNEY GENERAL AUTHORITY.—Upon receiving notice under paragraph (2), the Attorney General shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation of this Act or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1) nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths and affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1931 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

SEC. 404. RELATION TO STATE LAWS.

(a) IN GENERAL.—Except as provided in subsection (b), this title does not annul, alter, affect, or exempt any person subject to the provisions of this title from complying with the laws of any State with respect to security programs for personally identifiable information, except to the extent that those laws are inconsistent with any provisions of this title, and then only to the extent of such inconsistency.

(b) EXCEPTIONS.—No requirement or prohibition may be imposed under the laws of any State with respect to any subject matter regulated under section 401(c), relating to entities exempted from compliance with subtitle A.

Subtitle B—Security Breach Notification

SEC. 421. RIGHT TO NOTICE OF SECURITY BREACH.

(a) IN GENERAL.—Unless delayed under section 422(d) or exempted under section 424, any business entity or agency engaged in interstate commerce that involves collecting, accessing, using, transmitting, storing, or disposing of personally identifiable information shall notify, following the discovery of a security breach of its systems or databases in its possession or direct control when such security breach impacts sensitive personally identifiable information—

(1) if the security breach impacts more than 10,000 individuals nationwide, impacts a database, networked or integrated databases, or other data system associated with more than 1,000,000 individuals nationwide, impacts databases owned or used by the Federal Government, or involves sensitive personally identifiable information of employees and contractors of the Federal Government—

(A) the United States Secret Service, which shall be responsible for notifying——

(i) the Federal Bureau of Investigation, if the security breach involves espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service under section 3056(a) of title 18, United States Code; and

(ii) the United States Postal Inspection Service, if the security breach involves mail fraud; and

(B) the attorney general of each State affected by the security breach;

(2) each consumer reporting agency described in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a), pursuant to subsection (b); and

(3) any resident of the United States whose sensitive personally identifiable information was subject to the security breach, pursuant to sections 422 and 423, but in the event a business entity or agency is unable to identify the specific residents of the United States whose sensitive personally identifiable information was impacted by a security breach, the business entity or agency shall consult with the United States Secret Service to determine the scope of individuals who there is a reasonable basis to conclude have been impacted by such breach and should receive notice.

(b) CONSUMER REPORTING AGENCIES.—Any business entity or agency obligated to provide notice of a security breach to more than 1,000 residents of the United States under subsection (a)(3) shall inform consumer reporting agencies of the fact and scope of such notices for the purpose of facilitating and managing potential increases in consumer inquiries and mitigating identity theft or other negative consequences of the breach.

SEC. 422. NOTICE PROCEDURES.

(a) TIMELINESS OF NOTICE.—

(1) IN GENERAL.—Except as provided in subsection (c), all notices required under section 421 shall be issued expeditiously and without unreasonable delay after discovery of the events requiring notice.

(2) 14-DAY RULE.—The notices to Federal law enforcement and the attorney general of each State affected by a security breach required under section 421(a) shall be delivered not later than 14 days after discovery of the events requiring notice.

(3) REQUIRED DISCLOSURE.—In complying with the notices required under section 421, a business entity or agency shall expeditiously and without unreasonable delay take reasonable measures which are necessary to—

(A) determine the scope and assess the impact of a breach under section 421; and

(B) restore the reasonable integrity of the data system.

(b) METHOD.—Any business entity or agency obligated to provide notice under section 421 shall be in compliance with that section if they provide notice as follows:

(1) WRITTEN NOTIFICATION.—By written notification to the last known home address of the individual whose sensitive personally identifiable information was breached, or if unknown, notification via telephone call to the last known home telephone number.

(2) INTERNET POSTING.—If more than 1,000 residents of the United States require notice under section 421 and if the business entity or agency maintains an Internet site, conspicuous posting of the notice on the Internet site of the business entity or agency.

(3) MEDIA NOTICE.—If more than 5,000 residents of a State or jurisdiction are impacted, notice to major media outlets serving that State or jurisdiction.

(c) DELAY OF NOTIFICATION FOR LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—If Federal law enforcement or the attorney general of a State determines that the notices required under section 421(a) would impede a criminal investigation, such notices may be delayed until such law enforcement agency determines that the notices will no longer compromise such investigation.

(2) EXTENDED DELAY OF NOTIFICATION FOR LAW ENFORCEMENT PURPOSES.—If a business entity or agency has delayed the notices required under paragraphs (2) and (3) of section 421(a) as described in paragraph (1), the business entity or agency shall give notice 30 days after the day such law enforcement delay was invoked unless Federal law enforcement provides written notification that further delay is necessary.

SEC. 423. CONTENT OF NOTICE.

(a) IN GENERAL.—A business entity or agency obligated to provide notice to residents of the United States under section 421(a)(3) shall clearly and concisely detail the nature of the sensitive personally identifiable information impacted by the security breach.

(b) CONTENT OF NOTICE.—A notice under subsection (a) shall include—

(1) the availability of victim protection assistance pursuant to section 425;

(2) guidance on how to request that a fraud alert be placed in the file of the individual

maintained by consumer reporting agencies, pursuant to section 605A of the Fair Credit Reporting Act (15 U.S.C. 1681c–1) and the implications of such actions;

(3) the availability of a summary of rights for identity theft victims from consumer reporting agencies, pursuant to section 609 of the Fair Credit Reporting Act (15 U.S.C. 1681g);

(4) if applicable, notice that the State where an individual resides has a statute that provides the individual the right to place a security freeze on their credit report; and

(5) if applicable, notice that consumer reporting agencies have been notified of the security breach.

(c) MARKETING NOT ALLOWED IN NOTICE.—A notice under subsection (a) may not include—

(1) marketing information;

(2) sales offers; or

(3) any solicitation regarding the collection of additional personally identifiable information from an individual.

SEC. 424. RISK ASSESSMENT AND FRAUD PREVENTION NOTICE EXEMPTIONS.

(a) RISK ASSESSMENT EXEMPTION.—A business entity will be exempt from the notice requirements under paragraphs (2) and (3) of section 421(a), if a risk assessment conducted in consultation with Federal law enforcement and the attorney general of each State affected by a security breach concludes that there is a de minimis risk of harm to the individuals whose sensitive personally identifiable information was at issue in the security breach.

(b) FRAUD PREVENTION EXEMPTION.—A business entity will be exempt from the notice requirement under section 421(a) if—

(1) the nature of the sensitive personally identifiable information subject to the security breach cannot be used to facilitate transactions or facilitate identity theft to further transactions with another business entity that is not the business entity subject to the security breach notification requirements of section 421;

(2) the business entity utilizes a security program reasonably designed to block the use of the sensitive personally identifiable information to initiate unauthorized transactions before they are charged to the account of the individual; and

(3) the business entity has a policy in place to provide notice and provides such notice after a breach of the security of the system has resulted in fraud or unauthorized transactions, but does not necessarily require notice in other circumstances.

SEC. 425. VICTIM PROTECTION ASSISTANCE.

Any business entity or agency obligated to provide notice to residents of the United States under section 421(a)(3) shall offer to those same residents to cover the cost of—

(1) monthly access to a credit report for a period of 1 year from the date of notice provided under section 421(a)(3); and

(2) credit-monitoring services for up to 1 year from the date of notice provided under section 421(a)(3).

SEC. 426. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—Any business entity that violates the provisions of sections 421 through 425 shall be subject to civil penalties of not more than $5,000 per violation per day, with a maximum of $55,000 per day, while such violations persist.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A business entity that intentionally or willfully violates the provisions of sections 421 through 425 shall be subject to additional penalties in the amount of $5,000 per violation per day, with a maximum of an additional $55,000 per day, while such violations persist.

(3) EQUITABLE RELIEF.—A business entity engaged in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are cumulative and shall not affect any other rights and remedies available under law.

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—Whenever it appears that a business entity or agency to which this subtitle applies has engaged, is engaged, or is about to engage, in any act or practice constituting a violation of this subtitle, the Attorney General may bring a civil action in an appropriate district court of the United States to—

(A) enjoin such act or practice;

(B) enforce compliance with this subtitle; and

(C) obtain damages—

(i) in the sum of actual damages, restitution, and other compensation on behalf of the affected residents of a State; and

(ii) punitive damages, if the violation is willful or intentional; and

(D) obtain such other relief as the court determines to be appropriate.

(2) OTHER INJUNCTIVE RELIEF.—Upon a proper showing in the action under paragraph (1), the court shall grant a permanent injunction or a temporary restraining order without bond.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been, or is threatened to be, adversely affected by a violation of this subtitle, the State, as parens patriae, may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that practice;

(B) enforce compliance with this subtitle;

(C) obtain damages—

(i) in the sum of actual damages, restitution, and other compensation on behalf of the affected residents of that State; and

(ii) punitive damages, if the violation is willful or intentional; and

(D) obtain such other equitable relief as the court may consider to be appropriate.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXCEPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION WHEN PRACTICABLE.—In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Attorney General at the time the attorney general of a State files the action.

(3) ATTORNEY GENERAL AUTHORITY.—Upon receiving notice under paragraph (2), the Attorney General shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation of this Act or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this subsection shall be construed to prevent an attorney general of a State from exercising the powers conferred on such attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

SEC. 427. RELATION TO STATE LAWS.

(a) IN GENERAL.—Except as provided in subsection (b), this title does not annul, alter, affect, or exempt any person subject to the provisions of this title from complying with the laws of any State with respect to protecting consumers from the risk of theft or misuse of personally identifiable information, except to the extent that those laws are inconsistent with any provisions of this title, and then only to the extent of such inconsistency.

(b) EXCEPTIONS.—No requirement or prohibition may be imposed under the laws of any State with respect to any subject matter regulated under—

(1) section 3(9), relating to the definition of ''security breach'';

(2) paragraphs (1)(A), (2), and (3) of subsection (a), and subsection (b) of section 421, relating to the right to notice of security breach;

(3) section 422, relating to notice procedures;

(4) section 423, relating to notice content, except that nothing in this section shall prevent a State from requiring notice of additional victim protection assistance by that State; and

(5) section 424, relating to risk assessment and fraud prevention notice exemptions.

SEC. 428. STUDY ON SECURING PERSONALLY IDENTIFIABLE INFORMATION IN THE DIGITAL ERA.

(a) REQUIREMENT FOR STUDY.—Not later than 120 days after the date of enactment of this Act, the Department of Justice shall enter into a contract with the National Research Council of the National Academies to conduct a study on securing personally identifiable information in the digital era.

(b) MATTERS TO BE ASSESSED IN REVIEW.—The study required under subsection (a) shall include—

(1) threats to the public posed by the unauthorized or improper disclosure of personally identifiable information, including threats to—

(A) law enforcement;

(B) homeland security;

(C) individual citizens; and

(D) commerce;

(2) an assessment of the benefits and costs of currently available strategies for securing

personally identifiable information based on—

(A) technology;

(B) legislation;

(C) regulation; or

(D) public education;

(3) research needed to develop additional strategies;

(4) recommendations for congressional or other policy actions to further minimize vulnerabilities to the threats described in paragraph (1); and

(5) other relevant issues that in the discretion of the National Research Council warrant examination.

(c) TIME LINE FOR STUDY AND REQUIREMENT FOR REPORT.—Not later than 18-month period beginning upon completion of the performance of the contract described in subsection (a), the National Research Council shall conduct the study and report its findings, conclusions, and recommendations to Congress.

(d) FEDERAL DEPARTMENT AND AGENCY COMPLIANCE.—Federal departments and agencies shall comply with requests made by the National Science Foundation, National Research Council, and National Academies for information that is necessary to assist in preparing the report required by subsection (c).

(e) AUTHORIZATION OF APPROPRIATIONS.—Of the amounts authorized to be appropriated to the Department of Justice for Department-wide activities, $850,000 shall be made available to carry out the provisions of this section for fiscal year 2006.

SEC. 429. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated such sums as may be necessary to cover the costs incurred by the United States Secret Service to carry out investigations and risk assessments of security breaches as required under this subtitle.

SEC. 430. EFFECTIVE DATE.

This subtitle shall take effect 90 days after the date of enactment of this Act.

TITLE V—PROTECTION OF SOCIAL SECURITY NUMBERS

SEC. 501. SOCIAL SECURITY NUMBER PROTECTION.

(a) IN GENERAL.—No person may—

(1) display any individual's social security number to a third party without the voluntary and affirmatively expressed consent of such individual; or

(2) sell or purchase any social security number of an individual without the voluntary and affirmatively expressed consent of such individual.

(b) PREREQUISITES FOR CONSENT.—To obtain the consent of an individual under paragraphs (1) or (2) of subsection (a), the person displaying, selling, or attempting to sell, purchasing, or attempting to purchase the social security number of such individual shall—

(1) inform such individual of the general purpose for which the social security number will be used, the types of persons to whom the social security number may be available, and the scope of transactions permitted by the consent; and

(2) obtain the affirmatively expressed consent (electronically or in writing) of such individual.

(c) HARVESTED SOCIAL SECURITY NUMBERS.—Subsection (a) shall apply to any public record of a Federal agency that contains social security numbers extracted from other public records for the purpose of displaying or selling such numbers to the general public.

(d) EXCEPTIONS.—Nothing in this section shall be construed to prohibit or limit the display, sale, or purchase of a social security number—

(1) as required, authorized, or excepted under Federal law;

(2) to the extent necessary for a public health purpose, including the protection of the health or safety of an individual in an emergency situation;

(3) to the extent necessary for a national security purpose;

(4) to the extent necessary for a law enforcement purpose, including the investigation of fraud and the enforcement of a child support obligation;

(5) to the extent necessary for research conducted for the purpose of advancing public knowledge, on the condition that the researcher provides adequate assurances that—

(A) the social security numbers will not be used to harass, target, or publicly reveal information concerning any individual;

(B) information about individuals obtained from the research will not be used to make decisions that directly affect the rights, benefits, or privileges of specific individuals; and

(C) the researcher has in place appropriate safeguards to protect the privacy and confidentiality of any information about individuals;

(6) if such a number is required to be submitted as part of the process for applying for any type of Federal, State, or local government benefit or program;

(7) when the transmission of the number is incidental to, and in the course of, the sale, lease, franchising, or merger of all or a portion of a business; or

(8) to the extent only the last 4 digits of a social security number are displayed.

SEC. 502. LIMITS ON PERSONAL DISCLOSURE OF SOCIAL SECURITY NUMBERS FOR COMMERCIAL TRANSACTIONS AND ACCOUNTS.

(a) IN GENERAL.—Part A of title XI of the Social Security Act (42 U.S.C. 1301 et seq.) is amended by adding the following:

"SEC. 1150A. LIMITS ON PERSONAL DISCLOSURE OF SOCIAL SECURITY NUMBERS FOR COMMERCIAL TRANSACTIONS AND ACCOUNTS.

''(a) ACCOUNT NUMBERS.—

''(1) IN GENERAL.—A business entity may not—

''(A) require an individual to use the social security number of such individual as an account number or account identifier when purchasing a commercial good or service; or

''(B) deny an individual goods or services for refusing to accept the use of the social security number of such individual as an account number or account identifier.

''(2) EXISTING ACCOUNT EXCEPTION.—Paragraph (1) shall not apply to any account number or account identifier established prior to the date of enactment of this Act.

''(b) SOCIAL SECURITY NUMBER PREREQUISITES FOR GOODS AND SERVICES.—A business entity may not require an individual to provide the social security number of such individual when purchasing a commercial good or service or deny an individual goods or services for refusing to provide that number except for any purpose relating to—

''(1) obtaining a consumer report for any purpose permitted under the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

''(2) a background check of the individual conducted by a landlord, lessor, employer, or voluntary service agency;

''(3) law enforcement; or

''(4) a Federal, State, or local law requirement.

''(c) APPLICATION OF CIVIL MONEY PENALTIES.—A violation of this section shall be deemed to be a violation of section 1129(a).

''(d) APPLICATION OF CRIMINAL PENALTIES.—A violation of this section shall be deemed to be a violation of section 208(a)(8).''.

SEC. 503. PUBLIC RECORDS.

(a) IN GENERAL.—Except as provided in paragraph (2), paragraphs (a) and (b) of section 501 shall apply to all public records posted on the Internet or provided in an electronic medium by, or on behalf of, a Federal agency.

(b) EXCEPTIONS.—

(1) TRUNCATION AND PRIOR DISPLAYS.—Section 501(a) shall not apply to—

(A) a public record which displays only the last 4 digits of the social security number of an individual; and

(B) any record or a category of public records first posted on the Internet or provided in an electronic medium by, or on behalf of, a Federal agency prior to the date of enactment of this Act.

(2) LAW ENFORCEMENT.—Nothing in this subsection shall be construed to prevent an entity acting pursuant to a police investigation or regulatory power of a domestic governmental unit from accessing the full social security number of an individual.

SEC. 504. TREATMENT OF SOCIAL SECURITY NUMBERS ON GOVERNMENT CHECKS AND PROHIBITION OF INMATE ACCESS.

(a) PROHIBITION OF USE OF SOCIAL SECURITY NUMBERS ON CHECKS ISSUED FOR PAYMENT BY GOVERNMENTAL ENTITIES.—

(1) IN GENERAL.—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)) is amended by adding at the end the following:

''(x) No Federal, State, or local agency may display the social security account number of any individual, or any derivative of such number, on any check issued for any payment by the Federal, State, or local agency.''.

(2) EFFECTIVE DATE.—The amendment made under paragraph (1) shall apply with respect to checks issued after the date that is 3 years after the date of enactment of this Act.

(b) PROHIBITION ON INMATE ACCESS TO SOCIAL SECURITY NUMBERS.—

(1) IN GENERAL.—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)), as amended by subsection (b), is further amended by adding at the end the following:

''(xi)(I) No Federal, State, or local agency may employ, or enter into a contract for the use or employment of, prisoners in any capacity that would allow such prisoners access to the social security account numbers of other individuals.

''(II) For purposes of this clause, the term 'prisoner' means an individual confined in a jail, prison, or other penal institution or correctional facility pursuant to conviction of such individual of a criminal offense.''.

(2) EFFECTIVE DATE.—The amendment made under paragraph (1) shall apply with respect to employment of prisoners, or entry into contract with prisoners, after the date that is 1 year after the date of enactment of this Act.

SEC. 505. STUDY AND REPORT.

(a) BY THE COMPTROLLER GENERAL.—The Comptroller General of the United States (in this section referred to as the ''Comptroller General'') shall conduct a study and prepare a report on—

(1) all of the uses of social security numbers permitted, required, authorized, or excepted under any Federal law; and

(2) the uses of social security numbers in Federal, State, and local public records.

(b) CONTENT OF REPORT.—The report required under subsection (a) shall—

(1) identify users of social security numbers under Federal law;

(2) include a detailed description of the uses allowed as of the date of enactment of this Act;

(3) describe the impact of such uses on privacy and data security;

(4) evaluate whether such uses should be continued or discontinued by appropriate legislative action;

(5) examine whether States are complying with prohibitions on the display and use of social security numbers—

(A) under the Privacy Act of 1974 (5 U.S.C. 552a et seq.); and

(B) the Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.);

(6) include a review of the uses of social security numbers in Federal, State, or local public records;

(7) include a review of the manner in which public records are stored (with separate reviews for both paper records and electronic records);

(8) include a review of the advantages, utility, and disadvantages of public records that contain social security numbers, including—

(A) impact on law enforcement;

(B) threats to homeland security; and

(C) impact on personal privacy and security;

(9) include an assessment of the costs and benefits to State and local governments of truncating, redacting, or removing social security numbers from public records, including a review of current technologies and procedures for truncating, redacting, or removing social security numbers from public records (with separate assessments for both paper and electronic records);

(10) include an assessment of the benefits and costs to businesses, non-profit organizations, and the general public of requiring truncation, redaction, or removal of social security numbers on public records (with separate assessments for both paper and electronic records);

(11) include an assessment of Federal and State requirements to truncate social security numbers, and issue recommendations on—

(A) how to harmonize those requirements; and

(B) whether to further extend truncation requirements, taking into consideration the impact on accuracy and use;

(12) include recommendations regarding whether subsection (a) should apply to any record or category of public records first posted on the Internet or provided in an electronic medium by, or on behalf of, a Federal agency prior to the date of enactment of this Act; and

(13) include such recommendations for legislation based on criteria the Comptroller General determines to be appropriate.

(c) REQUIRED CONSULTATION.—In developing the report required under this subsection, the Comptroller General shall consult with—

(1) the Administrative Office of the United States Courts;

(2) the Conference of State Court Administrators;

(3) the Department of Justice;

(4) the Department of Homeland Security;

(5) the Social Security Administration;

(6) Sate and local governments that store, maintain, or disseminate public records; and

(7) other stakeholders, including members of the private sector who routinely use public records that contain social security numbers.

(d) TIMING OF REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General shall report to Congress its findings under this section.

SEC. 506. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—Any person that violates the provisions of sections 501 or 502 shall be subject to civil penalties of not more than $5,000 per violation per day, with a maximum of $35,000 per day, while such violations persist.

(2) INTENTIONAL OR WILLFUL VIOLATION.—Any person who intentionally or willfully violates the provisions of sections 501 or 502 shall be subject to additional penalties in the amount of $5,000 per violation per day, with a maximum of an additional $35,000 per day, while such violations persist.

(3) EQUITABLE RELIEF.—Any person who engages in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are cumulative and shall not affect any other rights and remedies available under law

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—Whenever it appears that a person to which this title applies has engaged, is engaged, or is about to engage, in any act or practice constituting a violation of this title, the Attorney General may bring a civil action in an appropriate district court of the United States to—

(A) enjoin such act or practice;

(B) enforce compliance with this title; and

(C) obtain damages—

(i) in the sum of actual damages, restitution, and other compensation on behalf of the affected residents of a State; and

(ii) punitive damages, if the violation is willful or intentional; and

(D) obtain such other relief as the court determines to be appropriate.

(2) OTHER INJUNCTIVE RELIEF.—Upon a proper showing in the action under paragraph (1), the court shall grant a permanent injunction or a temporary restraining order without bond.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by an act or practice that violates this section, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this Act;

(C) obtain damages, restitution, or other compensation on behalf of residents of that State; or

(D) obtain such other legal and equitable relief as the court may consider to be appropriate.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Attorney General—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Attorney General as soon after the filing of the complaint as practicable.

(3) ATTORNEY GENERAL AUTHORITY.—Upon receiving notice under paragraph (2), the Attorney General shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation of this Act or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths and affirmations;

(C) or compel the attendance of witnesses or the production of documentary and other evidence.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

SEC. 507. RELATION TO STATE LAWS.

(a) IN GENERAL.—Except as provided in subsection (b), this title does not annul, alter, affect, or exempt any person subject to the provisions of this title from complying with the laws of any State with respect to protecting and securing social security numbers, except to the extent that those laws are inconsistent with any provisions of this title, and then only to the extent of such inconsistency.

(b) EXCEPTIONS.—No requirement or prohibition may be imposed under the laws of any State with respect to any subject matter regulated under—

(1) section 501(b), relating to prerequisites for consent for the display, sale, or purchase of social security numbers;

(2) section 501(c), relating to harvesting of social security numbers; and

(3) section 504, relating to treatment of social security numbers on government checks and prohibition of inmate access.

TITLE VI—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL DATA

SEC. 601. GENERAL SERVICES ADMINISTRATION REVIEW OF CONTRACTS.

(a) IN GENERAL.—In considering contract awards entered into after the date of enactment of this Act, the Administrator of the General Services Administration shall evaluate—

(1) the program of a contractor to ensure the privacy and security of data containing personally identifiable information;

(2) the compliance of a contractor with such program;

(3) the extent to which the databases and systems containing personally identifiable information of a contractor have been compromised by security breaches; and

(4) the response by a contractor to such breaches, including the efforts of a contractor to mitigate the impact of such breaches.

(b) PENALTIES.—In awarding contracts for products or services related to access, use, compilation, distribution, processing, analyzing, or evaluating personally identifiable information, the Administrator of the General Services Administration shall include the following:

(1) Monetary or other penalties—

(A) for failure to comply with subtitles A and B of title IV of this Act;

(B) if a contractor knows or has reason to know that the personally identifiable information being provided is inaccurate, and provides such inaccurate information; or

(C) if a contractor is notified by an individual that the personally identifiable information being provided is inaccurate and it is in fact inaccurate.

(2) Accuracy update requirements that obligate a contractor to provide notice to the Federal department or agency of any changes or corrections to the personally identifiable information provided under the contract.

SEC. 602. REQUIREMENT TO AUDIT INFORMATION SECURITY PRACTICES OF CONTRACTORS AND THIRD PARTY BUSINESS ENTITIES.

Section 3544(b) of title 44, United States Code, is amended—

(1) in paragraph (7)(C)(iii), by striking ''and'' after the semicolon;

(2) in paragraph (8), by striking the period and inserting ''; and''; and

(3) by adding at the end the following:

''(9) procedures for evaluating and auditing the information security practices of contractors or third party business entities supporting the information systems or operations of the agency involving personally identifiable information, and ensuring remedial action to address any significant deficiencies.''.

SEC. 603. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT USE OF COMMERCIAL INFORMATION SERVICES CONTAINING PERSONALLY IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Section 208(b)(1) of the E-Government Act of 2002 (44 U.S.C. 3501 note) is amended—

(1) in subparagraph (A)(i), by striking ''or''; and

(2) in subparagraph (A)(ii), by striking the period and inserting ''; or''; and

(3) by inserting after clause (ii) the following:

''(iii) purchasing or subscribing for a fee to personally identifiable information from a commercial entity (other than news reporting or telephone directories).''.

(b) LIMITATION.—Notwithstanding any other provision of law, commencing 60 days after the date of enactment of this Act, no Federal department or agency may procure or access any commercially available database consisting primarily of personally identifiable information concerning United States persons (other than news reporting or telephone directories) unless the head of such department or agency—

(1) completes a privacy impact assessment under section 208 of the E-Government Act of 2002 (44 U.S.C. 3501 note), which shall include a description of—

(A) such database;

(B) the name of the commercial entity from whom it is obtained; and

(C) the amount of the contract for use;

(2) adopts regulations that specify—

(A) the personnel permitted to access, analyze, or otherwise use such databases;

(B) standards governing the access analysis, or use of such databases;

(C) any standards used to ensure that the personally identifiable information accessed, analyzed, or used is the minimum necessary to accomplish the intended legitimate purpose of the Federal department or agency;

(D) standards limiting the retention and redisclosure of personally identifiable information obtained from such databases;

(E) procedures ensuring that such data meet standards of accuracy, relevance, completeness, and timeliness;

(F) the auditing and security measures to protect against unauthorized access, analysis, use, or modification of data in such databases;

(G) applicable mechanisms by which individuals may secure timely redress for any adverse consequences wrongly incurred due to the access, analysis, or use of such databases;

(H) mechanisms, if any, for the enforcement and independent oversight of existing or planned procedures, policies, or guidelines; and

(I) an outline of enforcement mechanisms for accountability to protect individuals and the public against unlawful or illegitimate access or use of databases; and

(3) incorporates into the contract or other agreement with the commercial entity, provisions—

(A) providing for penalties—

(i) if the entity knows or has reason to know that the personally identifiable information being provided to the Federal department or agency is inaccurate, and provides such inaccurate information; or

(ii) if the entity is notified by an individual that the personally identifiable information being provided to the Federal department or agency is inaccurate and it is in fact inaccurate; and

(B) requiring commercial entities to inform Federal departments or agencies to which they sell, disclose, or provide access to personally identifiable information of any changes or corrections to the personally identifiable information.

(c) INDIVIDUAL SCREENING PROGRAMS.—Notwithstanding any other provision of law, commencing 60 days after the date of enactment of this Act, no Federal department or agency may use commercial databases to implement an individual screening program unless such program is—

(1) congressionally authorized; and

(2) subject to regulations developed by notice and comment that—

(A) establish a procedure to enable individuals, who suffer an adverse consequence because the screening system determined that they might pose a security threat, to appeal such determination and correct information contained in the system;

(B) ensure that Federal and commercial databases that will be used to establish the identity of individuals or otherwise make assessments of individuals under the system will not produce a large number of false positives or unjustified adverse consequences;

(C) ensure the efficacy and accuracy of all of the search tools that will be used and ensure that the department or agency can make an accurate predictive assessment of those who may constitute a threat;

(D) establish an internal oversight board to oversee and monitor the manner in which the system is being implemented;

(E) establish sufficient operational safeguards to reduce the opportunities for abuse;

(F) implement substantial security measures to protect the system from unauthorized access;

(G) adopt policies establishing the effective oversight of the use and operation of the system; and

(H) ensure that there are no specific privacy concerns with the technological architecture of the system.

(d) STUDY OF GOVERNMENT USE.—

(1) SCOPE OF STUDY.—Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall conduct a study and audit and prepare a report on Federal agency use of commercial databases, including the impact on privacy and security, and the extent to which Federal contracts include sufficient provisions to ensure privacy and security protections, and penalties for failures in privacy and security practices.

(2) REPORT.—A copy of the report required under paragraph (1) shall be submitted to Congress.

SEC. 604. IMPLEMENTATION OF CHIEF PRIVACY OFFICER REQUIREMENTS.

(a) DESIGNATION OF THE CHIEF PRIVACY OFFICER.—Pursuant to the requirements under section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Division H of Public Law 108–447; 118 Stat. 3199) that each agency designate a Chief Privacy Officer, the Department of Justice shall implement such requirements by designating a department-wide Chief Privacy Officer, whose primary role shall be to fulfill the duties and responsibilities of Chief Privacy Officer and who shall report directly to the Deputy Attorney General.

(b) DUTIES AND RESPONSIBILITIES OF CHIEF PRIVACY OFFICER.—In addition to the duties and responsibilities outlined under section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Division H of Public Law 108–447; 118 Stat. 3199), the Department of Justice Chief Privacy Officer shall—

(1) oversee the Department of Justice's implementation of the requirements under section 603 to conduct privacy impact assessments of the use of commercial data containing personally identifiable information by the Department;

(2) promote the use of law enforcement technologies that sustain, rather than erode, privacy protections, and assure that the implementation of such technologies relating to the use, collection, and disclosure of personally identifiable information preserve the privacy and security of such information; and

(3) coordinate with the Privacy and Civil Liberties Oversight Board, established in the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458), in implementing paragraphs (1) and (2) of this subsection.

Mr. LEAHY. Mr. President, today we introduce the Specter-Leahy Personal Data Privacy and Security Act of 2005. Reforms are urgently needed to protect Americans' privacy and to secure their personal data. There have been steady waves of security breaches over the past 6 months, with the latest involving a database containing 40 million credit card numbers at a company that most Americans never knew existed.

These security breaches are a window on a broader, more challenging trend. Advanced technologies have improved our lives and can help make us safer. Private data about Americans has become a hot commodity. This personal and financial information about each of us suddenly is a treasure trove, valuable and vulnerable, but our privacy and security laws have not kept pace. The reality is that in the digital era, a robust market has developed for collecting and selling personal information. Today, all types of corporate and governmental entities routinely traffic in billions of digitized personal records about Americans.

The data broker market has exploded in size to meet this demand. Insecure databases are now low-hanging fruit for hackers looking to steal identities and commit fraud. We are seeing a rise

in organized rings that target personal data to sell in online, virtual bazaars.

In this information-saturated age, the use of personal data has significant consequences for every American. People have lost jobs, mortgages and control over their credit and identities because personal information has been mishandled or listed incorrectly. This trend raises new threats to our personal security as well as to our privacy. In one disturbing case, a stalker purchased the Social Security number of a woman with whom he was obsessed, used that information to track her down. He killed her, and then shot himself.

Americans everywhere are wondering, ''Why do all these companies have my personal information? What are they doing with it? Why aren't they protecting it better?'' And they are right to wonder. It is time for Congress to catch up with the data market and to show the American people that we are aware of these threats and will protect the privacy and security of their personal information.

Chairman SPECTER and I have worked closely together over many months to craft comprehensive legislation to fix key vulnerabilities in our information economy. We thought through these issues carefully and took the time needed to develop well-balanced, focused legislation that provides strong protections where necessary. We also provide tough penalties and consequences for failing to protect Americans' most personal information. Reforms like these are long overdue. This issue and our legislation deserve to become a key part of this year's domestic agenda so that we can achieve some positive changes in areas that affect the everyday lives of Americans.

First, our bill requires data brokers to let people know what information they have about them, and to allow people to correct inaccurate information. These principles have precedent from the credit report context, and we have adapted them in a way that makes sense for the data brokering industry. It's a simple matter of fairness.

Second, we would require companies that have databases with personal information on Americans to establish and implement data privacy and security programs. Any company that wants to be trusted by the public in this day and age must vigilantly protect databases housing Americans' private data. They also have a responsibility in the next link in the security chain, to make sure that contractors hired to process data are on the up-and-up and secure. This is critical as Americans' personal information is increasingly processed overseas.

Third, our bill requires notice when sensitive personal information has been compromised. The American people have a right to know when they are at risk because of corporate failures to protect their data, or when a criminal has infiltrated data systems. The notice rules in our bill were crafted carefully to ensure that the trigger for notice is tied to risk and to recognize important fraud prevention techniques that already exist. But our priority was making sure that victims have that critical information as a roadmap providing the assistance necessary to protect themselves, their families and their financial well-being.

Fourth, our bill provides tough new protections for Social Security numbers, which are the keys to unlocking so much of our financial and personal lives. The use of Social Security numbers has expanded well beyond the intended purposes. Some uses provide important benefits, but others have made Americans vulnerable. Social Security numbers are for sale online for small fees. Earlier this year, it was reported that a payroll and benefits company put the Social Security numbers of 1,000 workers on postcards—on postcards—brazenly visible for anyone to see. Worse still, those postcards described in detail how those Social Security numbers could be used to access employee benefits online. This is unacceptable, and this bill would make that kind of disregard and sloppiness illegal.

Finally, our bill addresses the government's use of personal data. We are living in a world where the government is increasingly looking to the private sector to get personal data that it could not legally collect on its own without oversight and appropriate protections. So ingrained has the data broker-government partnership become that a ChoicePoint executive stated, ''We do act as an intelligence agency, gathering data, applying analytics.'' While these relationships can help protect us, there must be oversight and appropriate protections.

The recent decision to award ChoicePoint an IRS contract highlights this tension. It is especially galling right now to be rewarding firms that have been so careless with the public's confidential information. The dust has not yet settled and the investigations are incomplete on ChoicePoint's lax security practices. We should at least take a pause before rewarding such missteps with even more government contracts. This bill would place privacy and security front and center in evaluating whether data brokers can be trusted with government contracts that involve sensitive information about the American people. It would require contract reviews that include these considerations, audits to ensure good practice, and contract penalties for failure to protect data privacy and security.

The Specter-Leahy legislation meets other key goals. It provides tough monetary and criminal penalties for compromising personal data or failing to provide necessary protections. This creates an incentive for companies to protect personal information, especially when there is no commercial relationship between individuals and companies using their data.

Our legislation also carefully balances the need for Federal uniformity and State leadership. States are often on the forefront of protecting privacy and spurring change. The California security breach law has been an important lesson. My State of Vermont was among the first—if not the first—to require individual consent before sharing financial information with third parties, and to require a person or business to obtain consent from individuals before reviewing their credit reports. The role of States is important, and our bill identifies areas that require uniformity while leaving the States free to act elsewhere as they see fit. We also would authorize an additional $100 million over 4 years to help state law enforcement fight misuse of personal information.

This is a solid bill—a comprehensive bill—that not only deals with providing Americans notice when they have already been hurt, but also deals with the underlying problem of lax security and lack of accountability in dealing with their most personal and private information.

I commend Senator SPECTER for his leadership on this emerging problem. A number of us have been working on these issues—Senator FEINSTEIN, Senator NELSON, Senator CANTWELL and Senator SCHUMER, among others. I appreciate and recognize their hard work and look forward to making progress together. I am pleased to work closely with Senator SPECTER on this and believe that we have a bill that significantly advances the ball in protecting Americans.

I ask unanimous consent that a copy of the bill be printed in the RECORD.

By Mr. CORNYN (for himself, Mrs. LINCOLN, Mrs. HUTCHISON, Mr. TALENT, Mr. SANTORUM, Mr. COLEMAN, Mr. ISAKSON, Mr. ROBERTS, Mr. BROWNBACK, Mr. BOND, Mr. HATCH, Mr. ALLARD, Mr. ALEXANDER, Mr. MARTINEZ, and Mr. PRYOR):

S. 1333. A bill to amend the Agricultural Marketing Act of 1946 to establish a voluntary program for country of origin labeling of meat, and for other purposes; to the Committee on Agriculture, Nutrition, and Forestry.

Mr. CORNYN. Mr. President, I rise today to introduce the Meat Promotion Act of 2005.

This legislation is long overdue. When implemented, it will help assist our producers of cattle, pork, and other livestock to market and promote their products as born and raised in the United States. This proposal provides an efficient and effective solution to the country-of-origin labeling dilemma.

The Meat Promotion Act of 2005 will benefit U.S. food producers by promoting American-grown foods. This bipartisan effort is widely supported by producers, processors, and retailers as a means to finally move country-of-origin labeling forward.

This legislation provides for USDA implementation of a labeling program

that will be similar to the many voluntary labeling programs that currently exist. Hundreds of programs that label products by region, state, and U.S. brand have already proven their value for producers and consumers alike. The Meat Promotion Act will put the marketplace in charge by allowing producers to meet consumer demand. Where that demand is demonstrated, more products labeled with country-of-origin will become available.

Country-of-origin labeling has been an issue in the Senate for quite awhile, and yet, after all this time, we're no closer to promoting U.S. products than we were a decade ago. In reviewing the storied history of this issue, it's clear that there is not a shortage of viewpoints. One view overwhelmingly vocalized is that U.S. producers of beef and pork want to market and promote their products as born and raised in the United States of America. They are proud of what they produce, and they should be: the U.S. produces the safest, most abundant food supply at the most affordable price, and our livestock producers want to capture the value they add to the market.

But just like every other debate in Washington, the debate over country-of-origin labeling has been about the means to accomplish the goal. It is not that we are fighting about whether or not promoting U.S. product is a good idea. We are fighting about how to do it. Some in the U.S. Senate and some around the country have said: ''If it isn't mandatory, it's not labeling,'' or that the current mandatory labeling law that passed in the 2002 Farm Bill is the only way labeling will work. I strongly disagree.

The current mandatory law is an example of a good idea gone awry. The warning signs of the negative impact of this law have long been on the horizon. On a number of occasions the Government Accountability Office published reports and studies, and testified before Congress about the burdens of mandatory country-of-origin labeling.

In 1999—3 years before the current mandatory labeling law was passed—GAO testified before Congress that ''There is going to be significant costs associated with compliance and enforcement'' of mandatory labeling. At that same hearing, a representative of the Clinton administration testified that ''There are a variety of regulatory regimes for country-of-origin labeling that could be adopted.''

In 2000, the GAO released another study indicating that ''U.S. Packers, processors, and grocers would, to the extent possible, pass their compliance costs back to their suppliers—U.S. cattle and sheep ranchers—in the form of lower prices or forward to consumers in the form of higher retail prices.''

As if that was not enough, again in 2000, the USDA under President Clinton released another report which stated: ''[C]ountry-of-origin labeling is certain to impose at least some costs on an industry which will either be passed back to producers in the form of lower prices or forward to consumers via higher prices. There would also be compliance and enforcement cost to the government. The extent of these costs would vary depending on the nature of the regulatory scheme and the amount of enforcement and compliance action.''

Yet despite the warning signs, the current law passed as part of the 2002 Farm Bill.

When USDA issued the proposed rule, it contained a cost-benefit analysis that said implementation could cost up to $4 billion—with no quantifiable benefit. The rule was followed by a letter from the Director of Office of Information and Regulatory Affairs, Dr. John Graham, which said ''this is one of the most burdensome rules to be reviewed by this administration.''

And so, I am not surprised by how upset many of my constituents are, and that they have come asked me to do something about the burdens this law imposes on them. They ask: ''How can something so popular, like marketing and promoting U.S. products be so expensive?'' I am introducing this bill to help relieve that burden.

There has to be a better way to market and promote U.S. products, and I believe the Meat Promotion Act of 2005 will provide a better solution.

Some have said that voluntary labeling is like a voluntary speed limit—that it won't work. On what basis do they make that claim? Products like Certified Angus Beef, Angus Pride, Rancher's Reserve; these are all labeled on a volunteer basis under existing USDA programs. If producers want to have their products labeled, then they should participate in a voluntary labeling program rather than impose a costly burden on entire segments of our Nation's economy.

Others have argued that this is about food safety. Let's not kid ourselves: country-of-origin labeling is a product-marketing program, period. The security of our Nation's food supply is assured by a science-based, food-safety inspection system, not by labeling programs. In fact, the mandatory labeling law exempts food service and poultry. If this debate is about food safety, why are all poultry and the majority of beef imports for foodservice allowed an exemption? These exemptions clearly demonstrate food safety is not at issue.

Some have also pointed to the mandatory labeling law now in effect on seafood and fish, saying that the sky has not fallen on those industries. That is subject to interpretation. GAO analysis of the seafood provisions of the mandatory labeling law shows that the seafood industry could face up to $89 million in start-up costs and up to $6.2 million in additional costs in year 10 of the program. Likewise, USDA estimated total recordkeeping at $44.6 million for the first year and $24.4 million in subsequent years. The Office of Management and Budget found the rule to be an ''economically significant'' regulatory action and USDA believes the rule would adversely affect—in a substantial way—a key sector of the economy. GAO B–294914.

What do these numbers mean in a practical way? It means that these expenses are paid for out of the pockets of hardworking Americans, to fund a program that could be more efficient, more effective, and less costly.

I stand with the livestock producers that want to market and promote the products they are proud to raise. I believe they should be able to market and promote their products as born, raised, and processed in the United States, and I believe the Meat Promotion Act of 2005 provides the most effective and efficient opportunity for them to do so, while adding value to their bottom line and helping the economy of rural America.

By Mr. BUNNING (for himself and Mr. STEVENS):

S. 1334. A bill entitled ''The Professional Sports Integrity and Accountability Act''; to the Committee on Commerce, Science, and Transportation and the Committee on Finance.

Mr. STEVENS. Mr. President, I am pleased to support the efforts of my colleague Senator BUNNING in holding professional sports leagues in the United States to a higher standard with respect to testing their athletes for performance-enhancing drugs. Senator BUNNING's bill, ''The Professional Sports Integrity and Accountability Act,'' is another step toward holding professional sports leagues accountable as custodians of our Nation's pastimes. I have cosponsored a similar bill with Senator MCCAIN, and I look forward to working with both of them in the effort to rid professional sports of performance-enhancing drugs and setting a positive example for our youth who are using these substances at an alarming rate.

Over the past few years, the Commerce Committee has taken a series of actions to review the issue of performance-enhancing drug use at all levels of athletic competition, professional and amateur. The results of that review have been alarming. The evidence is clear that an increasing number of young amateur and U.S. Olympic athletes are using these substances for a multitude of reasons, but primarily to enhance athletic performance. Some experts suggest that many of these young athletes seek to emulate their professional sports heroes and are drawn to whatever it takes to achieve similar athletic greatness. For those skeptics who question this link and doubt the powerful effect that athletes have on the lives of kids, I remind them of the five-fold increase in the sales of the steroid-like substance androstenedione—better known as ''andro''—that occurred after Mark McGwire admitted to using the substance in 1998 while chasing Major League Baseball's home run record.

Since then, the problem of harmful supplement use among children and teenagers has reached epidemic proportions.

In 2004, more than 300,000 high school students used anabolic steroids, which are scheduled as a controlled substances in the United States. Evidence shows that teenagers are using these substances not only for athletic performance enhancement, but also for vanity. Recent news reports have indicated that when surveyed, an estimated 5 percent of high school girls and 7 percent of middle school girls admitted using anabolic steroids at some point in their lives. Steroid use has doubled among high school students since the early 1990s.

The adverse health consequences associated with such use are indisputable. Medical experts warn that the effects on children and teenagers include stunted growth, scarring acne, hormonal imbalances, liver and kidney damage, as well as an increased risk of heart disease and stroke later in life. Psychologically, steroids have been associated with increased aggression, suicide, and a greater propensity to commit serious crimes.

Notwithstanding the dire health effects of anabolic steroids or steroid-like substances, the use of any performance-enhancing substance for the sole purpose of gaining a competitive edge over an opponent is unfair. Professional sports leagues must be held to the highest standard and be held accountable to their players, American consumers who pay to see a fair competition on the playing field, and the young athletes who are led by the example of professional athletes.

By Mr. DODD (for himself, Mr. KENNEDY, Mr. KERRY, and Mr. BINGAMAN):

S. 1335. A bill to amend title XVIII of the Social Security Act to preserve access to appeals before administrative law judges under the medicare program; to the Committee on Finance.

Mr. DODD. Mr. President, I rise today to introduce the Justice for Medicare Beneficiaries Act of 2005, legislation that will ensure that Medicare beneficiaries who are denied health-related benefits can appeal these denials in a meaningful way. Very simply, this initiative will ensure that Medicare beneficiaries have access to timely, impartial, and in-person hearings before Administrative Law Judges.

Sec. 931 of the Medicare Prescription Drug, Improvement, and Modernization Act requires the transfer of the Medicare appeals process from the Social Security Administration (SSA) to the Department of Health and Human Services (HHS). A proposed rule recently put forth indicates that current HHS plans to bring about this transfer will significantly and negatively affect Medicare beneficiaries' ability to seek redress from the denial of benefits such as access to prescription medicines, home health services, and services provided at skilled nursing facilities.

Specifically, the Administration's proposed transfer plan, slated to go into effect in only a handful of days on July 1, will reduce the number of sites where these appeal hearings can take place to four from the more than 140 sites currently operating nationwide. Today, Medicare beneficiaries that have filed coverage appeals are granted a hearing before an Administrative Law Judge (ALJ). Under the proposed transfer plan, Medicare beneficiaries will now have their hearings heard via video- or teleconference (VTC) and will only be allowed to appear in person by request and if HHS determines that ''special or extraordinary circumstances exist.'' Moreover, beneficiaries granted an in-person hearing would not be assured that their cases would be heard within the 90-day window currently mandated by law. Lastly, the proposed transfer plan will endanger the independence and impartiality of Administrative Law Judges by requiring them to defer to program guidance provided by the Centers for Medicare and Medicaid Services (CMS) rather than on the Medicare statute and regulations, as they currently do.

Central to our system of justice is the right of aggrieved parties to appear before an impartial judge in person to have their cases heard. Appearing face-to-face before an impartial trier of fact is the best way to ensure that a full and fair hearing occurs. In person hearings allow parties to fully make their case. At the same time, they allow judges to best evaluate the demeanor and condition of the parties, and other aspects of a case. The Administration's proposed rule transferring the Medicare appeals process from SSA to HHS greatly endangers this right by gutting the current practice of guaranteeing the right of Medicare beneficiaries to appear in person before an ALJ when having their appeals heard and instead will now presume that these hearings will be heard via video- or teleconference.

Often when we talk about the denial of Medicare benefits, we are talking about the denial of services that literally have the ability to save lives. Medicare provides a critical safety net for millions of elderly and disabled beneficiaries and the proposed transfer plan's almost wholesale reliance on novel VTC technology may endanger the ability of many Medicare beneficiaries to accurately and personally portray the severity of their own health conditions.

The Justice for Medicare Beneficiaries Act of 2005 will ensure those Medicare beneficiaries that have filed coverage appeals have access to timely, impartial, and in-person hearings before Administrative Law Judges. Specifically, this initiative will ensure that Medicare appeals will be heard in person before an ALJ, as they presently are. While all Medicare beneficiaries will be entitled to appear in person for their hearing, any beneficiary may choose to have their hearing heard via video- or teleconference.

The legislation that I introduce today is in no way designed to prevent the adoption of the promising technology represented by VTC. Rather, this initiative simply seeks to preserve the critically important ability of Medicare beneficiaries to appear before the very judges charged with hearing their coverage appeals. By preventing the great majority of Medicare beneficiaries from appearing in person before the judge hearing their Medicare appeals, the Administration's proposed plan will greatly harm their ability to accurately and completely present all of the facts relevant to their case. And while I understand that many Medicare beneficiaries will choose to have their appeals heard via either video- or teleconference, I believe that we must preserve for Medicare beneficiaries the ability to appear in person before a judge when their cases are heard.

The legislation will also require that all Medicare coverage appeal hearings, regardless of whether a Medicare beneficiary appears in person or chooses to appear via video- or teleconference, will be heard within 90 days as mandated by the Benefits Improvement and Protection Act of 2000. All Medicare beneficiaries deserve to have their appeals heard in a timely manner regardless of whether their cases are heard in person or via utilizing VTC technology.

The Justice for Medicare Beneficiaries Act will also address the Administration's plans to reduce the number of sites where Medicare appeal hearings may be heard in person from the more than 140 sites currently available to four. This legislation will require at least one site for the hearing of in-person Medicare appeals in each state, the District of Columbia, and territory, with the nation's five largest states featuring two hearing sites geographically distributed throughout the state.

Lastly, this legislation will ensure the independence and impartiality of Administrative Law Judges by relieving them of the proposed transfer plan's mandate to grant ''substantial deference'' to CMS program guidance. Medicare beneficiaries appealing coverage decisions should be fully confident that the judges deciding their appeals are bound only by the merits of their case and not undue pressure from agency of administration interference.

I want to thank Senators KENNEDY, KERRY, and BINGAMAN for joining me in sponsoring this important initiative. The Justice for Medicare Beneficiaries Act is also supported by a number of national and local organizations dedicated to preserving the continued ability of Medicare beneficiaries to access needed health care services. Endorsing the legislation that I introduce today are the Center for Medicare Advocacy located in my own state of Connecticut, the National Health Law Program, the National Senior Citizens Law Center, the Medicare Advocacy Project of Vermont Legal Aid, the Medicare Advocacy Project of Greater

Boston Legal Services, and the Senior Citizens' Law Office of Albuquerque, NM.

In Congress we far too rarely have the opportunity to stave off problems before they occur. Rather, too often we are forced to involve ourselves in matters only after they have already wreaked havoc on the lives of our constituents. With passage of the Justice for Medicare Beneficiaries Act of 2005, we have the opportunity to avoid the adverse impact that the Administration's proposed transfer plan will likely have on Medicare beneficiaries. This legislation will preserve for our nation's 41 million Medicare beneficiaries the ability to timely appear in person before judges who will impartially determine which health care services they're entitled to receive under Medicare. Medicare beneficiaries deserve no less than the vital protections offered by this act and I ask for the support of my colleagues for this critically important initiative.

By Mr. ENZI (for himself and Mr. BAUCUS):

S. 1337. A bill to restore fairness and reliability to the medical justice system and promote patient safety by fostering alternatives to current medical tort litigation, and for other purposes; to the Committee on Health, Education, Labor, and Pensions.

Mr. ENZI. Mr. President, I rise today along with my colleague Senator BAUCUS from Montana to introduce a bill that will help bring about a more reliable system of medical justice for all Americans.

In the last Congress, we had three robust debates on a critical issue—medical liability reform. Though a majority of the Members of this body wanted to begin working to pass legislation, we didn't have the 60 Senators necessary to invoke cloture and begin the real work on the bills. That was disappointing, because skyrocketing medical liability insurance premiums are forcing doctors to move their practices to States with better legal environments and lower premiums. This is endangering the availability of critical healthcare services in many areas of Wyoming and other states.

Throughout our debate, I heard many of my colleagues say that they wanted to work on this issue, but that they simply could not support the bill as it stood. While I disagreed with their positions then, I respected their opposition. I also trust that they sincerely wanted to help solve our Nation's medical liability and litigation crisis.

During those debates, I noticed something interesting. While we argued the ''pros and cons'' of the bills, no one stood up to defend our current system of medical litigation. In fact, even some of the lawyers in this body agreed that our medical litigation system needs reform.

Why didn't we hear anyone defend the merits of our current medical litigation system? It's because our system doesn't work. It simply doesn't work for patients or for healthcare providers.

Compensation to patients injured by healthcare errors is neither prompt nor fair. The randomness and delay associated with medical litigation does not contribute to timely, reasonable compensation for most injured patients. Some injured patients get huge jury awards, while many others get nothing at all.

Let's look at the facts. In 1991, a group of researchers published a study in the New England Journal of Medicine. The study, known as the Harvard Medical Practice Study, was the basis for the Institute of Medicine's estimate that nearly 100,000 people die every year from healthcare errors.

As part of their study, the researchers reviewed the medical records of a random sample of more than 31,000 patients in New York State. They matched those records with statewide data on medical malpractice claims. The researchers found that nearly 30 percent of injuries caused by medical negligence resulted in temporary disability, permanent disability or death. However, less than 2 percent of those who were injured by medical negligence filed a claim. These figures suggest that most people who suffer negligent injuries don't receive any compensation.

When a patient does decide to litigate, only a few recover anything. Only one of every ten medical malpractice cases actually goes to trial, and of those cases, plaintiffs win less than one of every five. In addition, patients who file suit and are ultimately successful must wait a long time for their compensation—the average length of a medical malpractice action filed in state court is about 30 months.

While the vast majority of malpractice cases that go to trial are settled before the court hands down a verdict, the settlements even then don't guarantee that patients are compensated fairly, particularly after legal fees are subtracted. Research shows that for every dollar paid in malpractice insurance premiums, about 40 cents in compensation is actually paid to the plaintiff—the rest goes for legal fees, court costs, and other administrative expenditures.

To sum up: most patients injured by negligence don't file claims or receive compensation. Few of those that do file claims and go to court recover anything, and those who are successful wait a long time for their compensation. And those who settle out of court end up receiving only 40 cents for every dollar that healthcare providers pay in liability insurance premiums.

It's hard to say that our medical litigation system does right by patients in light of those facts. Unfortunately, our system doesn't work for healthcare providers either.

Earlier, I spoke about those Harvard researchers who found that fewer than 2 percent of those who were injured by medical negligence even filed a claim. As they reviewed the medical records for their study, the researchers also found another interesting fact—most of the providers against whom claims were eventually filed were not negligent at all.

That's right—most providers who were sued had not committed a negligent act.

In matching the records they reviewed to data on malpractice claims, the Harvard researchers found 47 actual malpractice claims. In only 8 of the 47 claims did they find evidence that medical malpractice had caused an injury. Even more amazingly, the physician reviewers found no evidence of any medical injury, negligent or not, in 26 of the 47 claims. However, 40 percent of these cases where they found no evidence of negligence nonetheless resulted in a payment by the provider. Basically, the researchers found no positive relationship between medical negligence and compensation.

That study was based on 1984 data. The same group of researchers conducted another study in Colorado and Utah in 1992, and they found the same thing. As in the 1984 study, they found that only 3 percent of patients who suffered an injury as a result of negligence actually sued. And again, physician reviewers could not find negligence in most of the cases in which lawsuits were filed.

Now, I assume that the patients who sued had either an adverse medical outcome, or at least an outcome that was less satisfactory than the patient expected. But our medical litigation system is not supposed to compensate patients for adverse outcomes or dissatisfaction—it's supposed to compensate patients who are victims of negligent behavior. It's supposed to be a deterrent to substandard medical care.

It's not fair to doctors and hospitals that they must pay to defend against meritless lawsuits. Nor is it fair that they must face a choice between settling for a small sum, even if they aren't at fault, so that they avoid getting sucked into the whirlpool of our medical litigation system.

It's not hard to understand why physicians and hospitals and their insurers want to stay out of court. When they lose, the decisions are increasingly resulting in mega-awards based on subjective ''non-economic'' damages. The number of awards exceeding $1 million grew by 50 percent between the periods of 1994–1996 and 1999–2000. Today, more than half of all jury awards exceed $1 million.

As a result, when a patient suffers a bad outcome and sues, providers have an incentive to settle the case out of court, even if the provider isn't at fault. But is this how our medical litigation system is supposed to work—as a tool for shaking down our healthcare providers?

Let's face it—our medical litigation system is broken. It doesn't work for

patients or providers. Even worse, it replaces the trust in the provider-patient relationship with distrust.

Then, when courts and juries render verdicts with huge awards that bear no relation to the conduct of the defendants, this destabilizes the insurance markets and sends premiums skyrocketing. This forces many physicians to curtail, move or drop their practices, leaving patients without access to necessary medical care. This is a particular problem in states like Wyoming, where we traditionally struggle with recruiting doctors and other healthcare providers.

Perhaps we could live with this flawed system if litigation served to improve quality or safety, but it doesn't. Litigation discourages the exchange of critical information that could be used to improve the quality and safety of patient care. The constant threat of litigation also drives the inefficient, costly and even dangerous practice of ''defensive medicine.''

Yes, indeed, defensive medicine is dangerous. A recent study found that one of every 1200 children who receive a CAT scan may die later in life from radiation-induced cancer. Knowing this puts a physician faced with anxious parents in a difficult situation. Does the doctor use his or her professional judgment and tell the parents of a sick child not to worry, or does the doctor order the CAT scan and subject the child to radiation that is probably unnecessary, just to provide some protection against a possible lawsuit?

We have a medical litigation system in which many patients who are hurt by negligent actions receive no compensation for their loss. Those who do receive compensation end up with about 40 cents of every premium dollar after legal fees and other costs are subtracted. And the likelihood and the outcomes of lawsuits and settlements bear little relation to whether or not a healthcare provider was at fault.

We like to say that justice is blind. With respect to our medical litigation system, I would say that justice is absent and nowhere to be found.

During our debates in the last Congress, I said that the current medical liability crisis and the shortcomings of our medical litigation system make it clear that it is time for a major change. I also said that regardless of how we voted, we all should work toward replacing the current medical tort liability scheme with a more reliable and predictable system of medical justice.

Today, Senator BAUCUS and I are introducing a bill that would help achieve that goal.

Most of us are familiar with the report on medical errors from the Institute of Medicine, also known as the IOM. Many of us may be less familiar with another report that the IOM published in 2003. That report is called ''Fostering Rapid Advances in Healthcare: Learning from System Demonstrations.''

Our Secretary of Health and Human Services at that time, Tommy Thompson, challenged the IOM to identify bold ideas that would challenge conventional thinking about some of the most vexing problems facing our healthcare system. In response, an IOM committee developed this report, which identified a set of demonstration projects that committee members felt would break new ground and yield a very high return-on-investment in terms of dollars and health.

Medical liability was one of the areas upon which the IOM committee focused. The IOM suggested that the federal government should support demonstration projects in the states. These demonstrations should be based on ''replacing tort liability with a system of patient-centered and safety-focused non-judicial compensation.''

The bill we are introducing today is in the spirit of this IOM report. This bill, the Fair and Reliable Medical Justice Act, would authorize funding for States to create demonstration programs to test alternatives to current medical tort litigation.

The funding to States under this bill would cover planning grants for developing proposals based on the models or other innovative ideas. Funding to States would also include the initial costs of getting the alternatives up and running.

The Fair and Reliable Medical Justice Act would require participating states and the Federal Government to collaborate in continuous evaluations of the results of the alternatives as compared to traditional tort litigation. This way, all States and the federal government can learn from new approaches.

By funding demonstration projects, I believe Congress could enable States to experiment with and learn from ideas that could provide long-term solutions to the current medical liability and litigation crisis.

In introducing this bill, I wanted to provide some alternative ideas that would contribute to the debate. As a result, the bill describes three models to which states could look in designing their alternatives.

For instance, a State could provide healthcare providers and organizations with immunity from lawsuits if they disclose an error that results in an injury and make a timely offer to compensate an injured patient for his or her actual net economic loss, plus a payment for pain and suffering if experts deem such a payment to be appropriate. This could give a healthcare provider who makes an honest mistake the chance to make amends financially with a patient, without the provider fearing that their honesty would land them in a lawsuit.

Another idea would be for a state to set up classes of avoidable injuries and a schedule of compensation for them, and then establish an administrative board to resolve claims related to those injuries. A scientifically rigorous process of identifying preventable injuries and setting appropriate compensation would be preferable to the randomness of the current system.

Still another option would be for a state to establish a special healthcare court for adjudicating medical malpractice cases. For this idea to work, the State would need to ensure that the presiding judges have expertise in and an understanding of healthcare, and allow them to make binding rulings on issues like causation compensation, and standards of care.

We already have specialized courts for complicated issues like taxes and highly charged issues like substance abuse and domestic violence. With all the flaws in our current medical litigation system, perhaps we should consider special courts for the complex and emotional issue of medical malpractice.

I believe one thing in our medical liability debate is absolutely clear—people are demanding change. The States are debating liability reform, and a number of states have enacted new laws. States are heeding this call for change, and Congress should support those efforts.

My own State, Wyoming, had had a number of lively legislative debates on medical liability reform over the past few years, but we have a constitutional amendment that prohibits limits on the amounts that can be recovered through lawsuits. The Wyoming Senate has considered bills recently to amend our State's constitution to create a commission on healthcare errors. That commission would have the power to review claims, decide if healthcare negligence had occurred, and determine the compensation for the death or injury according to a schedule or formula provided by law.

According to the key sponsor of these bills, Senator Charlie Scott, one of the biggest obstacles to passage is the uncertainty surrounding this new idea. No one has any basis for knowing what a proper schedule or formula for compensation would be. No one knows how much the system might cost, or how much injured patients would recover compared to what they recover now.

Senator Scott wrote me to say that federal support for finding answers to these questions might help the bill's sponsors sufficiently respond to the legitimate concerns of their fellow Wyoming legislators. We should be helping state legislators like Senator Scott develop thoughtful and innovative ideas such as the one he has proposed. That's one of the reasons I am offering this bill.

Clearly, the American people and their elected representatives have identified the need to reform our current medical litigation system. There is a real medical liability crisis, and Congress needs to act sooner rather than later.

My cosponsor Senator BAUCUS and I voted differently on medical liability reform in the last Congress, but we

both agree that we ought to lend a hand to States that are working to change their current medical litigation systems and to develop creative alternatives that could work much better for patients and providers. The States have been policy pioneers in many areas—workers' compensation, welfare reform, and electricity deregulation, to name three. Medical litigation should be the next item on the agenda of the laboratories of democracy that are our 50 States.

No one questions the need to restore reliability to our medical justice system. But how do we begin the process? One way is to foster innovation by encouraging States to develop more rational and predictable methods for resolving healthcare injury claims. And that is what the Fair and Reliable Medical Justice Act aims to do.

In the long run, we would all be better off with a more reliable system of medical justice than we have today. I know that my fellow Senators recognize this, so I hope my colleagues on both sides of the aisle will work with me and Senator BAUCUS on this legislation.

I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the bill was ordered to be printed in the RECORD, as follows:

S. 1337

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Fair and Reliable Medical Justice Act''.

SEC. 2. PURPOSES.

The purposes of this Act are—

(1) to restore fairness and reliability to the medical justice system by fostering alternatives to current medical tort litigation that promote early disclosure of health care errors and provide prompt, fair, and reasonable compensation to patients who are injured by health care errors;

(2) to promote patient safety through early disclosure of health care errors; and

(3) to support and assist States in developing such alternatives.

SEC. 3. STATE DEMONSTRATION PROGRAMS TO EVALUATE ALTERNATIVES TO CURRENT MEDICAL TORT LITIGATION.

Part P of title III of the Public Health Service Act (42 U.S.C. 280g et seq.) is amended by adding at the end the following:

''SEC. 3990. STATE DEMONSTRATION PROGRAMS TO EVALUATE ALTERNATIVES TO CURRENT MEDICAL TORT LITIGATION.

''(a) IN GENERAL.—The Secretary is authorized to award demonstration grants to States for the development, implementation, and evaluation of alternatives to current tort litigation for resolving disputes over injuries allegedly caused by health care providers or health care organizations.

''(b) DURATION.—The Secretary may award up to 10 grants under subsection (a) and each grant awarded under such subsection may not exceed a period of 5 years.

''(c) CONDITIONS FOR DEMONSTRATION GRANTS.—

''(1) REQUIREMENTS.—Each State desiring a grant under subsection (a) shall—

''(A) develop an alternative to current tort litigation for resolving disputes over injuries allegedly caused by health care providers or health care organizations that may be 1 of the models described in subsection (d); and

''(B) promote a reduction of health care errors by allowing for patient safety data related to disputes resolved under subparagraph (A) to be collected and analyzed by organizations that engage in voluntary efforts to improve patient safety and the quality of health care delivery.

''(2) ALTERNATIVE TO CURRENT TORT LITIGATION.—Each State desiring a grant under subsection (a) shall demonstrate how the proposed alternative described in paragraph (1)(A)—

''(A) makes the medical liability system more reliable through prompt and fair resolution of disputes;

''(B) encourages the early disclosure of health care errors;

''(C) enhances patient safety; and

''(D) maintains access to liability insurance.

''(3) SOURCES OF COMPENSATION.—Each State desiring a grant under subsection (a) shall identify the sources from and methods by which compensation would be paid for claims resolved under the proposed alternative to current tort litigation, which may include public or private funding sources, or a combination of such sources. Funding methods shall to the extent practicable provide financial incentives for activities that improve patient safety.

''(4) SCOPE.—

''(A) IN GENERAL.—Each State desiring a grant under subsection (a) may establish a scope of jurisdiction (such as a designated geographic region, a designated area of health care practice, or a designated group of health care providers or health care organizations) for the proposed alternative to current tort litigation that is sufficient to evaluate the effects of the alternative.

''(B) NOTIFICATION OF PATIENTS.—A State proposing a scope of jurisdiction under subparagraph (A) shall demonstrate how patients would be notified that they are receiving health care services that fall within such scope.

''(5) PREFERENCE IN AWARDING DEMONSTRATION GRANTS.—In awarding grants under subsection (a), the Secretary shall give preference to States—

''(A) that have developed the proposed alternative through substantive consultation with relevant stakeholders; and

''(B) in which State law at the time of the application would not prohibit the adoption of an alternative to current tort litigation.

''(d) MODELS.—

''(1) IN GENERAL.—Any State desiring a grant under subsection (a) that proposes an alternative described in paragraph (2), (3), or (4) shall be deemed to meet the criteria under subsection (c)(2).

''(2) EARLY DISCLOSURE AND COMPENSATION MODEL.—In the early disclosure and compensation model, the State shall—

''(A) require that health care providers or health care organizations notify a patient (or an immediate family member or designee of the patient) of an adverse event that results in serious injury to the patient, and that such notification shall not constitute an acknowledgment or an admission of liability;

''(B) provide immunity from tort liability to any health care provider or health care organization that offers in good faith to pay compensation in accordance with this section to a patient for an injury incurred in the provision of health care services (limited to claims arising out of the same nucleus of operative facts as the injury, and except in cases of fraud related to the provision of health care services, or in cases of criminal or intentional harm);

''(C) set a limited time period during which a health care provider or health care organization may make an offer of compensation benefits under subparagraph (B), with consideration for instances where prompt recognition of an injury is unlikely or impossible;

''(D) require that the compensation provided under subparagraph (B) include—

''(i) payment for the net economic loss of the patient, on a periodic basis, reduced by any payments received by the patient under—

''(I) any health or accident insurance;

''(II) any wage or salary continuation plan; or

''(III) any disability income insurance;

''(ii) payment for the non-economic damages of the patient, if appropriate for the injury, based on a defined payment schedule developed by the State in consultation with relevant experts and with the Secretary in accordance with subsection (g); and

''(iii) reasonable attorney's fees;

''(E) not abridge the right of an injured patient to seek redress through the State tort system if a health care provider does not enter into a compensation agreement with the patient in accordance with subparagraph (B) or if the compensation offered does not meet the requirements of subparagraph (D) or is not offered in good faith;

''(F) permit a health care provider or health care organization that offers in good faith to pay compensation benefits to an individual under subparagraph (B) to join in the payment of the compensation benefits any health care provider or health care organization that is potentially liable, in whole or in part, for the injury; and

''(G) permit any health care provider or health care organization to contribute voluntarily in the payment of compensation benefits to an individual under subparagraph (B).

''(3) ADMINISTRATIVE DETERMINATION OF COMPENSATION MODEL.—

''(A) IN GENERAL.—In the administrative determination of compensation model—

''(i) the State shall—

''(I) designate an administrative entity (in this paragraph referred to as the 'Board') that shall include representatives of—

''(aa) relevant State licensing boards;

''(bb) patient advocacy groups;

''(cc) health care providers and health care organizations; and

''(dd) attorneys in relevant practice areas;

''(II) set up classes of avoidable injuries, in consultation with relevant experts and with the Secretary in accordance with subsection (g), that will be used by the Board to determine compensation under clause (ii)(II);

''(III) modify tort liability, through statute or contract, to bar negligence claims in court against health care providers and health care organizations for the classes of injuries established under subclause (II), except in cases of fraud related to an injury, or in cases of criminal or intentional harm;

''(IV) outline a procedure for informing patients about the modified liability system described in this paragraph and, in systems where participation by the health care provider, health care organization, or patient is voluntary, allow for the decision by the provider, organization, or patient of whether to participate to be made prior to the provision of, use of, or payment for the health care service;

''(V) provide for an appeals process to allow for review of decisions; and

''(VI) establish procedures to coordinate settlement payments with other sources of payment;

''(ii) the Board shall—

''(I) resolve health care liability claims for certain classes of avoidable injuries as determined by the State and determine compensation for such claims;

''(II) develop a schedule of compensation to be used in making such determinations that includes—

''(aa) payment for the net economic loss of the patient, on a periodic basis, reduced by any payments received by the patient under any health or accident insurance, any wage or salary continuation plan, or any disability income insurance;

''(bb) payment for the non-economic damages of the patient, if appropriate for the injury, based on a defined payment schedule developed by the State in consultation with relevant experts and with the Secretary in accordance with subsection (g); and

''(cc) reasonable attorney's fees; and

''(III) update the schedule under subclause (II) on a regular basis.

''(B) APPEALS.—The State, in establishing the appeals process described in subparagraph (A)(i)(V), may choose whether to allow for de novo review, review with deference, or some opportunity for parties to reject determinations by the Board and elect to file a civil action after such rejection. Any State desiring to adopt the model described in this paragraph shall indicate how such review method meets the criteria under subsection (c)(2).

''(C) TIMELINESS.—The State shall establish timeframes to ensure that claims handled under the system described in this paragraph provide for adjudication that is more timely and expedited than adjudication in a traditional tort system.

''(4) SPECIAL HEALTH CARE COURT MODEL.—In the special health care court model, the State shall—

''(A) establish a special court for the timely adjudication of disputes over injuries allegedly caused by health care providers or health care organizations in the provision of health care services;

''(B) ensure that such court is presided over by judges with health care expertise who meet applicable State standards for judges and who agree to preside over such court voluntarily;

''(C) provide authority to such judges to make binding rulings on causation, compensation, standards of care, and related issues with reliance on independent expert witnesses commissioned by the court;

''(D) provide for an appeals process to allow for review of decisions; and

''(E) at its option, establish an administrative entity similar to the entity described in paragraph (3)(A)(i)(I) to provide advice and guidance to the special court.

''(e) APPLICATION.—

''(1) IN GENERAL.—Each State desiring a grant under subsection (a) shall submit to the Secretary an application, at such time, in such manner, and containing such information as the Secretary may require.

''(2) REVIEW PANEL.—

''(A) IN GENERAL.—In reviewing applications under paragraph (1), the Secretary shall consult with a review panel composed of relevant experts appointed by the Comptroller General.

''(B) COMPOSITION.—

''(i) NOMINATIONS.—The Comptroller General shall solicit nominations from the public for individuals to serve on the review panel.

''(ii) APPOINTMENT.—The Comptroller General shall appoint, at least 11 but not more than 15, highly qualified and knowledgeable individuals to serve on the review panel and shall ensure that the following entities receive fair representation on such panel:

''(I) Patient advocates.

''(II) Health care providers and health care organizations.

''(III) Attorneys with expertise in representing patients and health care providers.

''(IV) Insurers.

''(V) State officials.

''(C) CHAIRPERSON.—The Comptroller General, or an individual within the Government Accountability Office designated by the Comptroller General, shall be the chairperson of the review panel.

''(D) AVAILABILITY OF INFORMATION.—The Comptroller General shall make available to the review panel such information, personnel, and administrative services and assistance as the review panel may reasonably require to carry out its duties.

''(E) INFORMATION FROM AGENCIES.—The review panel may request directly from any department or agency of the United States any information that such panel considers necessary to carry out its duties. To the extent consistent with applicable laws and regulations, the head of such department or agency shall furnish the requested information to the review panel.

''(f) REPORT.—Each State receiving a grant under subsection (a) shall submit to the Secretary a report evaluating the effectiveness of activities funded with grants awarded under such subsection at such time and in such manner as the Secretary may require.

''(g) TECHNICAL ASSISTANCE.—

''(1) IN GENERAL.—The Secretary shall provide technical assistance to the States awarded grants under subsection (a).

''(2) REQUIREMENTS.—Technical assistance under paragraph (1) shall include—

''(A) the development of a defined payment schedule for non-economic damages (including guidance on the consideration of individual facts and circumstances in determining appropriate payment), the development of classes of avoidable injuries, and guidance on early disclosure to patients of adverse events; and

''(B) the development, in consultation with States, of common definitions, formats, and data collection infrastructure for States receiving grants under this section to use in reporting to facilitate aggregation and analysis of data both within and between States.

''(3) USE OF COMMON DEFINITIONS, FORMATS, AND DATA COLLECTION INFRASTRUCTURE.—States not receiving grants under this section may also use the common definitions, formats, and data collection infrastructure developed under paragraph (2)(B).

''(h) EVALUATION.—

''(1) IN GENERAL.—The Secretary, in consultation with the review panel established under subsection (e)(2), shall enter into a contract with an appropriate research organization to conduct an overall evaluation of the effectiveness of grants awarded under subsection (a) and to annually prepare and submit a report to the appropriate committees of Congress. Such an evaluation shall begin not later than 18 months following the date of implementation of the first program funded by a grant under subsection (a).

''(2) CONTENTS.—The evaluation under paragraph (1) shall include—

''(A) an analysis of the effect of the grants awarded under subsection (a) on the number, nature, and costs of health care liability claims;

''(B) a comparison of the claim and cost information of each State receiving a grant under subsection (a); and

''(C) a comparison between States receiving a grant under this section and States that did not receive such a grant, matched to ensure similar legal and health care environments, and to determine the effects of the grants and subsequent reforms on—

''(i) the liability environment;

''(ii) health care quality;

''(iii) patient safety; and

''(iv) patient and health care provider and organization satisfaction with the reforms.

''(i) OPTION TO PROVIDE FOR INITIAL PLANNING GRANTS.—Of the funds appropriated pursuant to subsection (k), the Secretary may use a portion not to exceed $500,000 per State to provide planning grants to such States for the development of demonstration project applications meeting the criteria described in subsection (c). In selecting States to receive such planning grants, the Secretary shall give preference to those States in which State law at the time of the application would not prohibit the adoption of an alternative to current tort litigation.

''(j) DEFINITIONS.—In this section:

''(1) HEALTH CARE SERVICES.—The term 'health care services' means any services provided by a health care provider, or by any individual working under the supervision of a health care provider, that relate to—

''(A) the diagnosis, prevention, or treatment of any human disease or impairment; or

''(B) the assessment of the health of human beings.

''(2) HEALTH CARE ORGANIZATION.—The term 'health care organization' means any individual or entity which is obligated to provide, pay for, or administer health benefits under any health plan.

''(3) HEALTH CARE PROVIDER.—The term 'health care provider' means any individual or entity—

''(A) licensed, registered, or certified under Federal or State laws or regulations to provide health care services; or

''(B) required to be so licensed, registered, or certified but that is exempted by other statute or regulation.

''(4) NET ECONOMIC LOSS.—The term 'net economic loss' means—

''(A) reasonable expenses incurred for products, services, and accommodations needed for health care, training, and other remedial treatment and care of an injured individual;

''(B) reasonable and appropriate expenses for rehabilitation treatment and occupational training;

''(C) 100 percent of the loss of income from work that an injured individual would have performed if not injured, reduced by any income from substitute work actually performed; and

''(D) reasonable expenses incurred in obtaining ordinary and necessary services to replace services an injured individual would have performed for the benefit of the individual or the family of such individual if the individual had not been injured.

''(5) NON-ECONOMIC DAMAGES.—The term 'non-economic damages' means losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship, loss of consortium (other than loss of domestic service), injury to reputation, and all other non-pecuniary losses of any kind or nature, to the extent permitted under State law.

''(k) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section such sums as may be necessary. Amounts appropriated pursuant to this subsection shall remain available until expended.''.

Mr. BAUCUS. Mr. President, I rise today to join Senator ENZI in introducing the Fair and Reliable Medical Justice Act of 2005. We have debated the medical liability issue in this chamber for years now. But the Senate has failed to take action to make the situation better. We need to deal with the issue of rising liability costs, and I think this bill is a good place to start.

One of my top priorities in the Senate is ensuring appropriate access to affordable, quality health care. In a rural State such as Montana, where health care providers are often few and far between, that is a tall order. It is a job that is made all the harder by rising medical liability insurance premiums.

To ensure proper access to care, we need to make certain that our health care providers can afford their medical liability insurance. We also need to make sure that patients who are harmed by medical mistakes have access to timely, reasonable compensation for their injuries.

The Fair and Reliable Medical Justice Act promotes the testing of alternatives to current medical tort liability litigation. It aims to increase the number of injured patients who receive compensation for their injuries, and make such compensation more accurate and more timely, all at lower administrative costs than current systems. The bill also encourages patient safety by promoting disclosure of medical errors, unlike the current system which does not encourage disclosure.

The Fair and Reliable Medical Justice Act would establish State-based demonstration programs to help States test alternative systems of health care-related dispute resolution under three different models: early disclosure and compensation; administrative determination of compensation; and special health care courts. Under the bill, states may develop other alternative plans for resolving health care related disputes as well.

The first model involves a system of early disclosure, which encourages providers to disclose medical errors that harm patients and offer just compensation for injuries. This model would maintain patients' access to the traditional legal system if claims cannot be resolved by early disclosure, or in cases resulting from criminal or intentional harm or fraud.

The second model would establish a board made up of providers and health care organizations, advocates, and attorneys. The board would establish classes of avoidable injuries and determine compensation rates for each, including economic and non-economic losses, and attorneys' fees.

The third model involves special health care courts, presided over by judges with special health care expertise, and assisted by independent experts. The judges would be subject to the same criteria as other State judges and sit on the court voluntarily.

These models are based on innovative efforts currently underway in the private sector and in some States, where success is already being achieved. I think it is time for us to try to encourage more innovation and expand the range of options being considered. State-based demonstrations provide a great setting for experimentation and learning. The Institute of Medicine suggested as much in its 2002 report entitled ''Fostering Rapid Advances in Health Care: Learning from System Demonstrations.''

I thank Senator ENZI for his leadership on this issue. I am proud to have worked with him to develop legislation that I believe will enhance patient safety. It is unacceptable that around 100,000 Americans die annually as a result of medical errors. And it is unacceptable that many patients hurt by medical errors receive no compensation for their injuries

This bill is a good opportunity for us to make progress on both fronts—to look at the medical liability issue from a new perspective, through a set of commonsense pilot projects centered on improving patient safety. I urge my colleagues to support this important effort.

By Ms. MURKOWSKI (for herself and Mr. STEVENS):

S. 1338. A bill to require the Secretary of the Interior, acting through the Bureau of Reclamation and the United States Geological Survey, to conduct a study on groundwater resources in the State of Alaska, and for other purposes; to the Committee on Energy and Natural Resources.

Ms. MURKOWSKI. Mr. President, I rise today to introduce a measure of benefit to my home State of Alaska, the Alaska Water Resources Act of 2005. The importance of water resource data collection to a State that has a resource-based economy cannot be overstated. Economic development is predicated on access to an adequate water supply, and in my State there is inadequate hydrologic data upon which to secure both economic development and the health and welfare of Alaskan citizens.

Alaska is an amazing State from a hydrological viewpoint. It is home to more than 3 million lakes—only about 100 being larger than 10 square miles—more than 12,000 rivers and uncounted thousands of streams, creeks and ponds. Together these water bodies hold about one-third of all the fresh water found in the United States.

Alaska is home to a number of large rivers. The Yukon, which originates in western Canada, runs 1,400 miles—discharging from 25,000 cubic feet of water per second in early spring to more than 600,000 cubic feet per second in May during the spring thaw. The Yukon drains roughly 330,000 square miles of Alaska and Canada, about one-third of the State. Besides the Yukon, Alaska is home to nine other major rivers and creeks all running more than 300 miles in length: the Porcupine, Koyukuk, Kuskokwim, Tanana, Innoko, Colville, Noatak, Kobuk and Birch Creek.

Alaska residents from early spring to fall face substantial flood threats, from spring flooding caused by breakup and ice damming to fall's heavy rains, but the State has fewer than 100 stream gaging stations operated by the U.S. Geological Survey—Alaska having less than 10 percent of the stream flow information that is taken for granted by all other States in the Nation. Alaska averages one working gage for each 10,000 square miles, while, as an example, Pacific Northwest States average one gage for each 365 square miles. To emphasize the lack of data now available for Alaska, I would point out that to equal the stream gage density of the Pacific Northwest States, my State would need to have over 1,600 total gage sites.

Alaska also supports the Nation's least modern and undeveloped potable water distribution system. Water for Alaska towns outside of the more densely populated ''Railbelt'' comes predominately from surface water sources Surface water sources often result in supply/storage problems since these surface sources freeze and are unavailable for up to half the year. The chances for water-borne contaminants to affect potable water supplies, including fecal matter from Alaska's plentiful wildlife populations, human waste from inadequate or nonexistent sewage treatment facilities, and natural mineral deposits (natural arsenic levels in mineralized zone creeks frequently exceeding EPA standards) are present and increasing. In areas that predominately depend on groundwater sources, such as the ''Railbelt,'' there is only very limited knowledge of the nature and extent of the aquifers that support those critical groundwater supplies. Extensive permafrost further complicates the potential for adverse impacts to Alaska. In portions of Southcentral Alaska where there is a dependence on groundwater as the source for an adequate healthy water supply, the availability of that supply is starting to be in jeopardy. Allocations of water need to be based on scientific data, and the data needed upon which the allocations are made is unavailable. Users of water are only beginning to realize the potential conflicts that may arise, and the limits on future economic development that may result from inadequate knowledge of the water resource, particularly in the Matanuska-Susitna Borough, on the Kenai Peninsula and to a lesser extent in portions of the Municipality of Anchorage where groundwater provided by wells is a crucial part of the State's water distribution system and where there is little known about the size, capacity, extent and recharge capability of the aquifers that these wells tap.

Alaska, according to the Alaska Department of Environmental Conservation, still has some 16,000 homes in 71 generally Native villages not being served by piped water or enclosed water haul systems. There are still 55 villages in Alaska where up to 29 percent of the residents are not served by sanitary water systems, with more than 60 percent of residents not being served in 16 villages. Even though since Statehood the State and Federal governments have spent $1.3 billion on rural water-sanitation system improvements in Alaska, the state has an estimated need for nearly $650 million in

additional funding to complete installation of a modern water-sanitation system.

Planning and engineering for those locations cannot be completed without better information as to the availability and extent of supply of water and better analysis of new technologies that could be used for water system installations, including possible desalination for some island and coastal communities.

For all these reasons, today I am introducing legislation authorizing the Department of the Interior's Commissioner of Reclamation and the Director of the U.S. Geological Survey to conduct a series of water resource studies in Alaska. The studies will include a survey of water treatment needs and technologies including desalination treatment, which may be applicable to the water resources development in Alaska. The study will review the need for enhancement of the National Streamflow Information Program administered by the U.S. Geological Survey. The Streamflow review will determine whether more stream gaging stations are necessary for flood forecasting, aiding resource extraction, determining the risk to the state's transportation system and for wildfire management. Groundwater resources will also be further evaluated and documented to determine the availability of water, the quality of that groundwater, and the extent of the aquifers in urban areas.

This type of study, already conducted for most all other Sates in the Nation, should help Alaska better plan and design water systems and transportation infrastructure and also better prepare for floods and summer wildfires.

There is literally ''water, water everywhere'' in Alaska, but too often, especially in communities such as Ketchikan that take water from surface sources, or the rapidly growing Mat-Su Valley, there may be less water to drink during unusually dry summers, There is a real and growing problem of maintaining an adequate supply of sufficient, pure water. This problem is only going to grow with a growing population and economy. This bill is designed to provide more information to help communities plan for future water needs and to help State officials plan for flood and fire safety concerns and economic development.

By Mr. LEAHY (for himself, Ms. COLLINS, Mr. JEFFORDS, Mrs. BOXER, Mr. KERRY, Mr. BIDEN, Ms. CANTWELL, Mr. CARPER, Mr. ROCKEFELLER, Mr. CORZINE, Mr. DAYTON, Mr. REID, Mr. DODD, Mrs. CLINTON, Mr. DURBIN, Mr. FEINGOLD, Mrs. FEINSTEIN, Mr. HARKIN, Mr. KENNEDY, Mr. KOHL, Mr. OBAMA, Mr. LAUTENBERG, Mr. LEVIN, Mr. LIEBERMAN, Ms. MIKULSKI, Mrs. MURRAY, Mr. REED, Mr. SARBANES, Mr. SCHUMER, Mr. WYDEN, Mr. AKAKA, and Ms. SNOWE):

S.J. Res. 20. A joint resolution disapproving a rule promulgated by the Administrator of the Environmental Protection Agency to delist coal and oil-direct utility units from the source category list under the Clean Air Act; to the Committee on Environment and Public Works.

Mr. LEAHY. Mr. President, along with Senator COLLINS and 28 of our colleagues, today I am introducing this resolution to halt the Bush administration's flawed and dangerous new rule on toxic mercury emissions. I am pleased that another leading cosponsor of this resolution is the ranking member of the Committee on Environment and Public Works, Senator JEFFORDS.

The Bush administration's new rule will continue to allow mercury, a substance so toxic that it causes birth defects and IQ loss, to continue to poison children and pregnant women. This disastrous rule should not be allowed to stand as the law of the land.

The bipartisan work that produced the Clean Air Act and the 1990 amendments established a process for us to begin cleaning up the toxic mercury spewing out of dirty power plants across the country. The 1990 amendments require the Environmental Protection Agency, EPA, to control each power plant's emissions of mercury and other toxics by 2008 at the latest. The act requires each plant to use the ''maximum achievable control technology'' on every generating unit. That is the law of the land. Anything less means more pollution.

But instead of working to enforce and implement the Clean Air Act, as two previous administrations had, the Bush administration has turned the Clean Air Act on its head. With this rule the administration revokes a 2000 EPA finding that it is ''necessary and appropriate'' to require that each power plant apply technology to reduce mercury emissions.

Let me repeat those plain, startling facts: By revoking the earlier EPA finding and deciding instead to coddle the biggest mercury polluters, the administration is saying it is no longer necessary or appropriate to adequately control mercury emissions. Although I am somewhat impressed that they can make this statement with straight faces, I am appalled at their audacious disregard for the health of the American people, and, like the scientific community, I am baffled by their gymnastic arguments.

The plain and simple truth is that this rule will allow more mercury into our environment than does the current law. Hundreds of the oldest, dirtiest power plants will not even control mercury emissions for more than a decade. That is what this rule gives us: More pollution, for longer than the Clean Air Act allows.

This rule is all the more shameful because the evidence of public health and environmental damage from mercury and other toxics is clear enough for action right now. We do not need to wait 10 or 20 years to know the facts about mercury's threats to human health. In fact EPA itself admits these threats. Look at EPA's own estimate of the number of newborns at risk of elevated mercury exposure, which has doubled to 630,000. EPA also found that 1 in 6 pregnant women has mercury levels in her blood above EPA's safe threshold. The National Academy of Sciences has confirmed scientific research showing that maternal consumption of unsafe levels of mercury in fish can cause neuro-developmental harm in children, resulting in learning disabilities, poor motor function, mental retardation, seizures and cerebral palsy.

Yet it seems the majority in Congress and this administration want to avoid any public daylight on this flawed rule. The Environment and Public Works Committee has refused to even hold a single hearing on this rule. Their aim is to keep the public in the dark, and I would guess that most Americans in fact do not yet know what EPA and the big polluters have been up to with this rule.

One reason for the administration's lack of candor clearly is the discovery that this rule has polluting industries' fingerprints all over it. EPA's first proposal for these rules lifted exact texts from memorandum provided by utility industry lobbyists. Another reason may be because the American people would find a process where the lobbyists are shut in and the public is shut out, where the scientific and economic analysis was manipulated, and where the public's health was ignored.

But the administration's arrogance does not stop there. EPA's own inspector general and the Government Accountability Office criticized almost every aspect of how EPA drafted this rule. Unfortunately, their recommendations to improve it were also ignored. So were more than 680,000 public comments—a record for any EPA rule. So were the comments of many state environment departments, attorneys general, doctors, educators, sportsmen groups and EPA's own advisory committees. And, although it should not come as a surprise after 4 years working with this administration, the comments of 45 Senate and 184 House members were also ignored.

Many of us in the Senate have spent the past 2 years—working with 3 different administrators—trying to make the administration follow the Clean Air Act and produce a rule that puts the public's health over the profits of special interests. A rule that heeds the science and encourages available technologies to solve this problem. They failed on all fronts, big time.

Instead they produced a rule that will do nothing for at least a decade, despite years of analysis by EPA showing the need for quick action. According to EPA's own regulatory impact analysis, we will be lucky if 1 percent of power plant capacity will have mercury controls by 2015, and only 3 percent by 2020.

As a Vermonter I know it is ''appropriate and necessary'' to limit the pollution plumes from grandfathered power plants. You cannot even see my state on EPA's maps showing mercury pollution because so much of it is being dumped on us from upwind power plants. Vermonters and New Englanders have been waiting for decades for EPA to take action so that our lakes can be cleaned up.

For all their talk of family values, the administration has yet again put the value of corporate contributions—not families—first. It is not a family value to tell a whole generation of women that their health is not important. It is not a family value to put another generation of young kids at risk of learning disabilities. These mercury rules do just that.

It is time to put people first, and to stop letting the big polluters and the special interests write the rules and run the show over at EPA.

This resolution will ensure that the health and safety of U.S. citizens are fully considered, before EPA rescinds its commitment to protect public health from the dangers of mercury pollution. To leave mercury pollution from power plants as the only source of toxic air pollution that is allowed to avoid rigorous emissions standards under the Clean Air Act is a risk to the public's health that we need not, and should not, accept.

I urge my colleagues to support this resolution.

SUBMITTED RESOLUTIONS

SENATE RESULTION 184—EXPRESSING THE SENSE OF THE SENATE REGARDING MANIFESTATIONS OF ANTI-SEMITISM BY UNITED NATIONS MEMBER STATES AND URGING ACTION AGAINST ANTI-SEMITISM BY UNITED NATIONS OFFICIALS, UNITED NATIONS MEMBER STATES, AND THE GOVERNMENT OF THE UNITED STATES, AND FOR OTHER PURPOSES

Mr. SANTORUM (for himself, Mr. FEINGOLD, Mr. SMITH, Ms. COLLINS, Mr. COLEMAN, and Mr. VOINOVICH) submitted the following resolution; which was referred to the Committee on Foreign Relations

S. RES. 184

Whereas the United Nations Universal Declaration of Human Rights recognizes that ''the inherent dignity and equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world'';

Whereas United Nations General Assembly Resolution 3379 (1975) concluded that ''Zionism is a form of racism and racial discrimination'' and the General Assembly, by a vote of 111 to 25, only revoked Resolution 3379 in 1991 in response to strong leadership by the United States and after Israel made its participation in the Madrid Peace Conference conditional upon repeal of the resolution;

Whereas during the 1991 session of the United Nations Commission on Human Rights, the Syrian Ambassador to the United Nations repeated the outrageous ''blood libel'' that Jews allegedly have killed non-Jewish children to make unleavened bread for Passover and, despite repeated interventions by the Governments of Israel and the United States, this outrageous lie was not corrected in the record of the Commission for many months;

Whereas in March 1997, the Palestinian observer at the United Nations Commission on Human Rights made the contemptible charge that the Government of Israel had injected 300 Palestinian children with HIV (the human immunodeficiency virus, the pathogen that causes AIDS) despite the fact that an Egyptian newspaper had printed a full retraction to its earlier report of the same charges, and the President of the Commission failed to challenge this baseless and false accusation despite the request of the Government of Israel that he do so;

Whereas Israel was denied membership in any regional grouping of the United Nations until the year 2000, which prevented it from being a candidate for any elected positions within the United Nations system until that time, and Israel continues to be denied the opportunity to hold a rotating seat on the Security Council and it is the only member of the United Nations never to have served on the Security Council although it has been a member of the organization for 56 years;

Whereas Israel continues to be denied the opportunity to serve as a member of the United Nations Commission on Human Rights because it has never been included in a slate of candidates submitted by a regional grouping, and Israel is currently the only member of the Western and Others Group in a conditional status limiting its ability to caucus with its fellow members of this regional grouping;

Whereas the United Nations has permitted itself to be used as a battleground for political warfare against Israel led by Arab states and others, and 6 of the 10 emergency sessions of the United Nations General Assembly have been devoted to criticisms of and attacks against Israel;

Whereas the goals of the 2001 United Nations World Conference Against Racism were undermined by hateful anti-Jewish rhetoric and anti-Israel political agendas, prompting both Israel and the United States to withdraw their delegations from the Conference;

Whereas in 2004, the United Nations Secretary General acknowledged at the first United Nations-sponsored conference on anti-Semitism, that: ''It is clear that we are witnessing an alarming resurgence of this phenomenon in new forms and manifestations. This time, the world must not—cannot—be silent.'';

Whereas in 2004, the United Nations General Assembly's Third Committee for the first time adopted a resolution on religious tolerance that includes condemnation of anti-Semitism and ''recognized with deep concern the overall rise in instances of intolerance and violence directed against members of many religious communities . . . including . . . anti-Semitism . . . '';

Whereas in 2005, the United Nations held an unprecedented session to commemorate the 60th anniversary of the liberation of the Auschwitz concentration camp;

Whereas democratic Israel is annually the object of nearly two dozen redundantly critical resolutions in the United Nations General Assembly, which rarely adopts resolutions relating to specific countries; and

Whereas the viciousness with which Israel is attacked and discriminated against at the United Nations should not be allowed to continue unchallenged: Now, therefore, be it

Resolved, That—

(1) the Senate—

(A) welcomes recent attempts by the United Nations Secretary General to address the issue of anti-Semitism;

(B) calls on the United Nations to officially and publicly condemn anti-Semitic statements made at all United Nations meetings and hold accountable United Nations member states that make such statements; and

(C) strongly urges the United Nations Educational, Scientific and Cultural Organization (UNESCO) to develop and implement education awareness programs about the Holocaust throughout the world as part of an effort to combat the rise in anti-Semitism and racial, religious, and ethnic intolerance; and

(2) it is the sense of the Senate that—

(A) the President should direct the United States Permanent Representative to the United Nations to continue working toward further reduction of anti-Semitic language and anti-Israel resolutions;

(B) the President should direct the Secretary of State to include in the Department of State's annual Country Reports on Human Rights Practices and annual Report on International Religious Freedom information on activities at the United Nations and its constituent bodies relating to anti-Semitism by each of the countries included in these reports; and

(C) the President should direct the Secretary of State to use projects funded through the Middle East Partnership Initiative and United States overseas broadcasts to educate Arab and Muslim countries about anti-Semitism, religious intolerance, and incitement to violence.

Mr. SANTORUM. Mr. President, I rise today to submit a resolution to express the sense of the Senate regarding manifestations of anti-Semitism by United Nations member states and to urge action against anti-Semitism by United Nations officials, United Nations member states, and the U.S. government. I am very pleased to be joined in this effort by Senators FEINGOLD, SMITH, COLLINS, COLEMAN, and VOINOVICH, who are original cosponsors of this legislation.

The past several years have revealed an upsurge in anti-Semitic violence around the world. We have seen incidences of it in Europe, the Middle East, and, unfortunately, even at the United Nations. While the United Nations Universal Declaration of Human Rights recognizes that ''the inherent dignity and equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world,'' there are numerous examples of anti-Semitism and anti-Israel actions at the U.N. and by member states.

Allow me to list some examples of anti-Semitic and anti-Israel bias that have been included in the resolution. Clearly false accusations have been made against the Jewish people and the government of Israel at the U.N. Commission on Human Rights. These lies were not corrected for months or, in some cases, ever. Israel also continues to be denied the opportunity to hold a rotating seat on the Security Council, despite the fact that it has been a member of the organization for 56 years. It is the only member of the U.N. to be denied this seat. It continues to be denied the opportunity to